



Bartel, A., & Dokchitser, T. (2015). Brauer relations in finite groups. *Journal of the European Mathematical Society*, 17(10), 2473-2512. <https://doi.org/10.4171/JEMS/563>

Peer reviewed version

License (if available):
CC BY-NC

Link to published version (if available):
[10.4171/JEMS/563](https://doi.org/10.4171/JEMS/563)

[Link to publication record in Explore Bristol Research](#)
PDF-document

This is the author accepted manuscript (AAM). The final published version (version of record) is available online via EMS at http://www.ems-ph.org/journals/show_abstract.php?issn=1435-9855&vol=17&iss=10&rank=3. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: <http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/>

BRAUER RELATIONS IN FINITE GROUPS

ALEX BARTEL¹ AND TIM DOKCHITSER²

ABSTRACT. If G is a non-cyclic finite group, non-isomorphic G -sets X, Y may give rise to isomorphic permutation representations $\mathbb{C}[X] \cong \mathbb{C}[Y]$. Equivalently, the map from the Burnside ring to the rational representation ring of G has a kernel. Its elements are called Brauer relations, and the purpose of this paper is to classify them in all finite groups, extending the Tornehave-Bouc classification in the case of p -groups.

CONTENTS

1. Introduction	2
1.1. Background and main result	2
1.2. Overview of the proof	4
1.3. Remarks and applications	4
1.4. Notation	7
2. First properties	7
3. Imprimitivity criteria	8
4. A characterisation in terms of quotients	11
5. Primitive relations in p -groups	12
6. Main reduction in soluble groups	13
7. Quasi-elementary groups	17
7.1. The kernel of the conjugation action	18
7.2. Some Brauer relations	21
7.3. Primitive relations with trivial K	26
7.4. Primitive relations with non-trivial K	28
8. Examples	35
9. An application to regulator constants	35
References	38

Accepted for publication in J. Eur. Math. Soc. on 22.09.2013

¹MATHEMATICS INSTITUTE, ZEEMAN BUILDING, UNIVERSITY OF WARWICK, COVENTRY CV4 7AL, UK

²DEPARTMENT OF MATHEMATICS, UNIVERSITY WALK, BRISTOL BS8 1TW, UK

E-mail addresses: a.bartel@warwick.ac.uk, tim.dokchitser@bristol.ac.uk.

2000 *Mathematics Subject Classification.* 19A22, 20B05, 20B10.

[s:intro](#)

1. INTRODUCTION

1.1. Background and main result. The Burnside ring $B(G)$ of a finite group G is the free abelian group on isomorphism classes of finite G -sets modulo the relations $[X] + [Y] = [X \amalg Y]$ and with multiplication $[X] \cdot [Y] = [X \times Y]$. There is a natural ring homomorphism from the Burnside ring to the rational representation ring of G ,

$$B(G) \longrightarrow R_{\mathbb{Q}}(G), \quad X \mapsto \mathbb{Q}[X].$$

The purpose of this paper is to describe its kernel.

Both the kernel and the cokernel have been studied extensively. The cokernel is finite of exponent dividing $|G|$ by Artin's induction theorem, and Serre remarked that it need not be trivial ([29] Exc. 13.4). It is trivial for p -groups [19, 27, 28] and it has been determined in many special cases [18, 8, 22].

Elements of the kernel $K(G)$ are called *Brauer relations* or *(G -)relations*. The most general result on $K(G)$ is due to Tornehave [33] (see [24, 2.4]) and Bouc [11], who independently described it for p -groups.

There is a bijection $H \mapsto G/H$ between conjugacy classes of subgroups of G and isomorphism classes of transitive G -sets, and we will write elements $\Theta \in B(G)$ as $\Theta = \sum_i n_i H_i$ using this identification. In this notation,

$$\Theta \in K(G) \iff \sum_i n_i \operatorname{Ind}_{H_i}^G \mathbf{1}_{H_i} = 0.$$

If we allow inductions of arbitrary 1-dimensional representations instead of just the trivial character, isomorphisms between sums of such inductions are called monomial relations. Deligne [13, §1] described all monomial relations in soluble groups, following Langlands [26]. For arbitrary finite groups, a generating set of monomial relations was given by Snaith [31].

Following the approach of Langlands, Deligne, Tornehave and Bouc, we consider a relation “uninteresting” if it is induced from a proper subgroup or lifted from a proper quotient of G (see §2). We call a relation *imprimitive* if it is a linear combination of such relations from proper subquotients and *primitive* otherwise, and we let $\operatorname{Prim}(G)$ denote the quotient of $K(G)$ by the subgroup of imprimitive relations. The motivation for this approach is that if one wants to prove a statement that holds for all Brauer relations, and if this statement behaves well under induction and inflation, then it is enough to prove it for primitive relations (see also §1.3).

In this paper we classify finite groups that have primitive relations and determine $\operatorname{Prim}(G)$:

thm:A

Theorem A. Let p and l denote prime numbers. A finite non-cyclic group G has a primitive relation if and only if either

- (1) G is dihedral of order $2^n \geq 8$; or
- (2) $G = (C_p \times C_p) \rtimes C_p$ is the Heisenberg group of order p^3 with $p \geq 3$; or
- (3) G is an extension

$$1 \longrightarrow S^d \longrightarrow G \longrightarrow Q \longrightarrow 1,$$

where S is simple, Q is quasi-elementary, the natural map $Q \rightarrow \text{Out } S^d$ is injective and, moreover, either

- (a) S^d is minimal among the normal subgroups of G
(for soluble G , this is equivalent to $G \cong \mathbb{F}_l^d \rtimes Q$ with \mathbb{F}_l^d a faithful irreducible representation of Q) or
- (b) $G = (C_l \rtimes P_1) \times (C_l \rtimes P_2)$ with cyclic (possibly trivial) p -groups P_i that act faithfully on $C_l \times C_l$ with $l \neq p$; or
- (4) $G = C \rtimes P$ is quasi-elementary, P is a p -group, $|C| = l_1 \cdots l_t > 1$ with $l_i \neq p$ distinct primes, the kernel $K = \ker(P \rightarrow \text{Aut } C)$ is trivial, or isomorphic to D_8 , or has normal p -rank one (see Proposition 5.2).
Moreover, writing $K_j = \bigcap_{i \neq j} \ker(P \rightarrow \text{Aut } C_{l_i})$, either
 - (a) $K = \{1\}$, $t > 1$, and all K_j have the same non-trivial image in the Frattini quotient of P ; or
 - (b) $K \cong C_p$, $P \cong K \times (P/K)$, and all K_j have the same two-dimensional image in the Frattini quotient of P ; or
 - (c) $|K| > p$ or P is not a direct product by K , and the graph Γ attached to G by Theorem 7.30 is disconnected.

For these groups, $\text{Prim}(G)$ is as follows. We write μ for the Möbius function.

Case	$\text{Prim}(G)$	Basis of $\text{Prim}(G)$
1	$\mathbb{Z}/2\mathbb{Z}$	$\Theta = H - H' + ZH' - ZH$, $H \cong C_2$ and $H' \cong C_2$ are non-conjugate non-central, $Z = Z(G) \cong C_2$
2	$(\mathbb{Z}/p\mathbb{Z})^p$	$\Theta_j = \langle y \rangle - \langle xy^j \rangle - \langle y, z \rangle + \langle xy^j, z \rangle$, $1 \leq j \leq p$, $G = \langle x, z \rangle \rtimes \langle y \rangle$, $z \in Z(G)$
3a	\mathbb{Z} if Q cyclic $\mathbb{Z}/p\mathbb{Z}$ else (Q p -quasi-elementary)	$\left. \begin{aligned} \Theta &= C_{p^k} - pQ - \mathbb{F}_l \rtimes C_{p^k} + pG \text{ if } d=1, Q=C_{p^{k+1}} \\ \Theta &= G - Q + \alpha(C_n - \mathbb{F}_l \rtimes C_n) + \beta(C_m - \mathbb{F}_l \rtimes C_m) \\ &\quad \text{if } d=1, Q=C_{mn}, \alpha m + \beta n = 1 \text{ (any such } m, n > 1) \\ \Theta &= G - Q + \sum_U (U \rtimes N_Q U - \mathbb{F}_l^d \rtimes N_Q U) \\ &\quad \text{if } d > 1; \text{ sum over } U \subset \mathbb{F}_l^d \text{ of index } l \text{ up to } G\text{-conjugacy} \\ \Theta &= \text{any relation of the form } G + \sum_{H \neq G} a_H H \end{aligned} \right\} \begin{aligned} &G \cong \mathbb{F}_l^d \rtimes Q \\ &\text{soluble} \\ &S \not\cong \mathbb{F}_l \end{aligned}$
3b	\mathbb{Z} if $Q = \{1\}$ $\mathbb{Z}/p\mathbb{Z}$ if $Q \neq \{1\}$ ($Q = P_1 \times P_2$)	
4a	$\mathbb{Z}/p\mathbb{Z}$	$\Theta = \sum_{U \leq C} \mu(U)(MU - M'U)$, $M, M' \leq P$ of index p with signatures $(1, \dots, 1), (0, \dots, 0)$, respectively (c.f. Prop. 7.19)
4b	$(\mathbb{Z}/p\mathbb{Z})^{p-2}$	$\Theta_i = \sum_{U \leq CK} \mu(U)(H_1 U - H_i U)$ for $1 < i < p$, $H_j \leq P$ of index p , $K \not\leq H_j$ and $(H_j \cap K_1)\Phi(P)/\Phi(P) = L_j$, L_j distinct lines in $K_1\Phi(P)/\Phi(P)$ other than $K\Phi(P)/\Phi(P)$, $1 \leq j < p$
4c	$(\mathbb{Z}/p\mathbb{Z})^{d-1}$ $d = \#$ connected components of Γ	$\Theta_i = \sum_{U \leq CC_p^z} \mu(U)(H_1 U - H_i U)$, $2 \leq i \leq d$, H_j any vertex in the j th connected component of Γ and $C_p^z \cong C_p \leq Z(K)$

1.2. Overview of the proof. Our analysis of finite groups follows a standard pattern

abelian — p -groups — quasi-elementary — soluble — all finite,

with a somewhat surprising twist that the difficulty of understanding primitive relations seems to decrease from the middle to the sides.

It is classical that the only abelian groups that have primitive relations are $G = C_p \times C_p$. On the opposite side, Solomon's induction theorem together with the fact that imprimitive relations form an ideal in the Burnside ring immediately allows us to deal with a large class of groups: if G has a proper non-quasi-elementary quotient, then G has no primitive relations (Corollary 3.10 and Theorem 4.3(3)). Similarly, using Theorem 4.2, we get the same conclusion when G has non-cyclic quasi-elementary quotients for two distinct primes $p \neq q$ (Theorem 4.3), and deduce Theorem A in the non-soluble case. This strategy was inspired by Deligne's work on monomial relations.

The p -group case and the soluble case are somewhat more involved. Our main tool for showing imprimitivity is the fact that in quasi-elementary groups, a relation $\sum n_H H$ with all H contained in a proper subgroup of G is imprimitive (Proposition 3.7). This is surprisingly useful. For instance, together with Bouc's 'moving lemma' ([11] Lemma 6.15) it gives an alternative proof of the Tornehave-Bouc classification in the p -group case (see §5). The classification of primitive relations in soluble groups that are not quasi-elementary is also not hard (see §6).

The most subtle case is that of quasi-elementary groups (§7). Recall that a p -quasi-elementary group is one of the form $G = C \rtimes P$ with P a p -group and C cyclic of order coprime to p . Assuming that such a G has a primitive relation, we analyse the kernel of the action of P on C (§7.1) and decompose all permutation representations of G explicitly into irreducible characters (§7.2). We show that $\text{Prim}(G)$ is generated by relations of the form

$$\Theta = \sum_{U \leq C \cdot Z(G)} \mu(|U|)(UH_1 - UH_2),$$

where $H_1, H_2 \leq G$ are of maximal size among those subgroups that intersect $C \cdot Z(G)$ trivially, unless $Z(G)$ is trivial, in which case H_1, H_2 are of index p in P . This already settles Theorem B below, but the remaining issue of primitivity of these generating relations is quite tricky. To show that Θ as above is imprimitive, it is not enough to show that it is neither lifted from a quotient nor induced from a subgroup, since Θ could be a sum of relations each of which is either lifted or induced. It becomes necessary to explicitly split the maximal size subgroups into classes in such a way that any relation involving two subgroups from different classes has to be primitive. This is the general spirit of sections 7.3 and 7.4, which complete the proof of Theorem A.

sec:applies

1.3. Remarks and applications. Note that for non-soluble groups in Theorem A(3a), $\text{Prim}(G)$ is generated by any relation $\Theta = \sum_H n_H H$ with $n_G = \pm 1$ (Theorem 4.3). An explicit construction of such a relation can be found in [31, Theorem 2.16(i)]. We note also that the relations in Theorem A for soluble groups are fairly canonical, see e.g. Remark 7.34.

One of the reasons one is interested in Brauer relations comes from number theory. In fact, the motivation for the Langlands-Deligne classification of monomial relations in soluble groups [26, 13] was to build a well-defined theory of ϵ -factors of Galois representations starting with one-dimensional characters; to do this, one needs to prove that the ϵ -factors of one-dimensional characters cancel in all monomial relations of local Galois groups.

If F/\mathbb{Q} is a Galois extension of number fields, arithmetic invariants of subfields $K \subset F$ may be viewed, via the Galois correspondence $K \leftrightarrow \text{Gal}(F/K)$, as functions of subgroups of $G = \text{Gal}(F/\mathbb{Q})$. Some functions, such as the discriminant $K \mapsto \Delta(K)$ extended to $B(G) \rightarrow \mathbb{Q}^\times$ by linearity, factor through the representation ring $R_{\mathbb{Q}}(G)$ and so cancel in all Brauer relations. On the other hand, the class number $h(K)$, the regulator $R(K)$ or the number of roots of unity $w(K)$ are not ‘representation-theoretic’, and do not cancel in general. However, their combination hR/w does, as it is the leading term of the Dedekind ζ -function $\zeta_K(s)$ at $s = 1$, and ζ -functions are representation-theoretic by Artin formalism for L -functions.

Thus, Brauer relations can provide non-trivial relationships between different arithmetic invariants, like the class numbers and the regulators of various intermediate fields. This point of view proved to be very fruitful to study class numbers and unit groups [10, 25, 34, 30], related Galois module structures [9, 3] and Mordell-Weil groups and other arithmetic invariants of elliptic curves and abelian varieties [16, 15, 2]. In a slightly different direction, a verification of the vanishing in Brauer relations of *conjectural* special values of L -functions can be regarded as strong evidence for the corresponding conjectures. This has been carried out in the case of the Birch and Swinnerton-Dyer conjecture in [16] and in the case of the Bloch-Kato conjecture in [12].

One concrete number-theoretic application of Brauer relations is the theory of ‘regulator constants’, used in the proof of the Selmer parity conjecture for elliptic curves over \mathbb{Q} [16], questions related to Selmer growth [15, 17, 2], and also to analyse unit groups and higher K -groups of number fields [3, 6]. The regulator constant $\mathcal{C}_\Theta(\Gamma) \in \mathbb{Q}^\times$ is an invariant attached to a $\mathbb{Z}[G]$ -module Γ and a Brauer relation Θ in G . For applications to elliptic curves the most important regulator constant is that of the trivial $\mathbb{Z}[G]$ -module $\Gamma = \mathbf{1}$, as it controls the l -Selmer rank of the curve over the ground field. For $\Theta = \sum n_H H$ it is simply

$$\mathcal{C}_\Theta(\mathbf{1}) = \prod_H |H|^{-n_H}.$$

To deduce something about the Selmer rank, one relies on Brauer relations in which this invariant, or rather its l -part, is non-trivial. As an application of Theorem A, in §9 we settle a question left unanswered in [16, 15, 17, 2], namely which groups have such a Brauer relation. This is done in Theorem 9.1 and Corollary 9.2; for an example of number theoretic consequences of this result, see [4].

For such applications one needs a collection of Brauer relations that span $K(G)$ and that are ‘as simple as possible’, but whether they are imprimitive is less important. Theorem A describes the *smallest* list of groups such that

all Brauer relations in all finite groups come¹ from such subquotients. Let us give an alternative version of the classification theorem with a much cleaner set of generating relations, that avoids the fiddly combinatorial conditions of Theorem A (especially 4a,4b,4c). It is a direct consequence of Theorem A.

thm:B

Theorem B. *All Brauer relations in soluble groups are generated by relations Θ from subquotients G of the following three types. In every case, G is an extension $1 \rightarrow C \rightarrow G \rightarrow Q \rightarrow 1$ with Q quasi-elementary and acting faithfully on C .*

- (1) $C = \mathbb{F}_l$, l a prime, (so $G = C \rtimes Q$), $H \leq G$ meets C trivially and

$$\Theta = [Q:H]G - [Q:H]Q + H - CH.$$

- (2) $C = \mathbb{F}_l^d$, with l a prime, $d \geq 2$, $G = C \rtimes Q$ and

$$\Theta = G - Q + \sum_U (U \rtimes N_Q U - \mathbb{F}_l^d \rtimes N_Q U),$$

the sum taken over representatives of G -conjugacy classes of subgroups $U \leq \mathbb{F}_l^d$ of index l .

- (3) C is cyclic, Q is an abelian p -group, $H_1, H_2 \leq G$ intersect C trivially, $|H_1| = |H_2|$, and

$$\Theta = \sum_{U \leq C} \mu(|U|)(UH_1 - UH_2).$$

Conversely, all $\Theta \in B(G)$ of the listed type are Brauer relations, not necessarily primitive. Finally, relations from subquotients of type (1), (3) and

- (2') $C = S^d$ with $d \geq 1$ and S simple, G is not quasi-elementary and

$$\Theta = \text{any relation of the form } G + \sum_{H \neq G} a_H H$$

generate all Brauer relations in all finite groups.

Acknowledgements. We are really fortunate to have had several extremely conscientious referees who made numerous corrections, pertinent remarks, and suggestions for improvement, and who we are very grateful to. We especially wish to thank the JEMS referee for an incredibly thorough reading of the manuscript.

The second author is supported by a Royal Society University Research Fellowship, and the first author was partially supported by the EPSRC and is partially supported by a Research Fellowship from the Royal Commission for the Exhibition of 1851. Parts of this research were done at St Johns College, Robinson College and DPMMS in Cambridge, CRM in Barcelona, and Postech University in Pohang. We would like to thank these institutions for their hospitality and financial support.

¹We would like to propose to use the word *indufted* instead of a vague ‘come’ or a cumbersome ‘induced and/or lifted’, but we were not brave enough to do this throughout the paper

1.4. Notation. Throughout the paper, G is a finite group; $Z(G)$ stands for the centre of G and $\Phi(G)$ for the Frattini subgroup; whenever $Z(G)$ is a cyclic p -group, we write C_p^z for the central subgroup of order p ; we denote by $\mathbf{1}$ the trivial representation; restriction from G to H and induction from H to G are denoted by $\text{Res}_H^G \rho$ and $\text{Ind}_H^G \sigma$, respectively; ${}^g H$ stands for gHg^{-1} .

s:first

2. FIRST PROPERTIES

Relations can be induced from and restricted to subgroups, and lifted from and projected to quotients as follows: let $\Theta = \sum_i n_i H_i$ be a G -relation.

- **Induction.** If G' is a group containing G , then, by transitivity of induction, Θ can be induced to a G' -relation $\text{Ind}^{G'} \Theta = \sum_i n_i H_i$.
- **Inflation.** If $G \cong \tilde{G}/N$, then each H_i corresponds to a subgroup \tilde{H}_i of \tilde{G} containing N , and, inflating the permutation representations from a quotient, we see that $\tilde{\Theta} = \sum_i n_i \tilde{H}_i$ is a \tilde{G} -relation.
- **Restriction.** If H is a subgroup of G , then by Mackey decomposition Θ can be restricted to an H -relation

$$\text{Res}_H \Theta = \sum_i \left(n_i \sum_{g \in H_i \backslash G/H} H \cap {}^g H_i \right).$$

On the level of G -sets this is simply the restriction of a G -set to H .

- **Projection (or deflation).** If $N \triangleleft G$, then $N\Theta = \sum_i N H_i$ is a G/N -relation.

Remark 2.1. Note that by definition of multiplication in the Burnside ring, $\Theta \cdot H = \text{Ind}^G(\text{Res}_H \Theta)$ for any G -relation Θ and any subgroup $H \leq G$.

The number of isomorphism classes of irreducible rational representations of a finite group G is equal to the number of conjugacy classes of cyclic subgroups of G (see [29, §13.1, Cor. 1]). Since the cokernel of $B(G) \rightarrow R_{\mathbb{Q}}(G)$ is finite (see [29, §13.1, Theorem 30]), the rank of the kernel $K(G)$ is the number of conjugacy classes of non-cyclic subgroups.

Explicitly, Artin's induction theorem gives a relation for each non-cyclic subgroup H of G ,

$$|H| \cdot \mathbf{1} = \sum_C n_C C, \quad n_C \in \mathbb{Z},$$

the sum taken over the cyclic subgroups of H . These are clearly linearly independent, and thus give a basis of $K(G) \otimes \mathbb{Q}$.

Example 2.2. Cyclic groups have no non-zero relations.

exer:G20

Example 2.3. Let $G = C_l \rtimes H$, with l prime and $H \neq \{1\}$ acting faithfully on C (so H is cyclic of order dividing $l-1$). Let \tilde{H} be any subgroup of H , set $\tilde{G} = C_l \rtimes \tilde{H}$. Then,

$$\tilde{H} - [H : \tilde{H}] \cdot H - \tilde{G} + [H : \tilde{H}] \cdot G$$

is a relation. This can be checked by a direct computation, using the explicit description of irreducible characters of G in Remark 6.3. (See e.g. Corollary 7.12.)

ex:cpcp

Example 2.4. Let $G = C_p \times C_p$. All its proper subgroups are cyclic, so $K(G)$ has rank one. It is generated by $\Theta = 1 - \sum_C C + pG$, with the sum running over all subgroups of order p , as can be checked by an explicit decomposition into irreducible characters, as above (or see [11] or Proposition 6.4 below).

s:imprim**lem:deflations**

3. IMPRIMITIVITY CRITERIA

Lemma 3.1. *Let G be a finite group, and $\Theta = \sum_i n_i H_i$ a G -relation in which each H_i contains some non-trivial normal subgroup N_i of G . Then Θ is imprimitive.*

Proof. Subtracting the projection onto N_1 , we get a relation

$$\Theta - N_1\Theta = \sum_{i, H_i \not\leq N_1} n_i (H_i - N_1 H_i),$$

which consists of subgroups each of which contains one of N_2, \dots, N_k . Repeatedly replacing Θ by $\Theta - N_j\Theta$ we see that the remaining relation is zero, so Θ is a sum of relations that are lifted from quotients. \square

lem:noncycliccentre

Lemma 3.2. *Let $G \not\cong C_p \times C_p$ be a finite group with non-cyclic centre. Then G has no primitive relations.*

Proof. Let $Z = C_p \times C_p \leq Z(P)$. For any $H \leq G$ that intersects Z trivially, $HZ/H \cong C_p \times C_p$. By lifting the relation of Example 2.4 to HZ and then inducing to G , we can replace any occurrence of H in any G -relation by groups that intersect Z non-trivially, using imprimitive relations. Each such intersection is normal in G , so by Lemma 3.1 the resulting relation is imprimitive as well. \square

We will now develop criteria for a relation to be induced from a subgroup.

prop:biggroupin

Proposition 3.3. *Let G be a finite group and $D \leq G$ a subgroup for which the natural map $B(D) \rightarrow B(G)$ is injective. If $\Theta = \sum_i n_i H_i$ is a G -relation with $H_i \leq D$ for all i , then Θ is induced from a D -relation.*

Proof. First, we claim that the image of $\text{Ind} : K(D) \rightarrow K(G)$ is a saturated sublattice², i.e. that if Θ is induced from a D -relation and R is a G -relation such that $\Theta = nR$ for some integer n , then R is induced from a D -relation (and not just from an element of the Burnside ring of D , which is trivially true). Indeed, it is enough to show that the image of the induction map $\text{Ind} : K(D) \rightarrow B(G)$ is saturated. But it is a composition of the two injections $K(D) \rightarrow B(D) \xrightarrow{\text{Ind}} B(G)$ whose images are clearly saturated, and so it has saturated image.

The image \mathcal{Y} of $\text{Ind} : K(D) \rightarrow K(G)$ is obviously contained in the space \mathcal{X} of G -relations $\sum_i n_i H_i$ for which $H_i \leq D$ for all i . So we only need to compare the ranks of the two spaces.

We have already remarked that the rank of $K(G)$ is equal to the number of conjugacy classes of non-cyclic subgroups of G . A basis for $K(G) \otimes \mathbb{Q}$ is obtained by applying Artin's induction theorem to a representative of each conjugacy class of non-cyclic subgroups of G . Hence, it is immediate that

²that is, $K(D) \rightarrow K(G)$ has torsion-free cokernel

a basis for $\mathcal{X} \otimes \mathbb{Q}$ is given by the subset of this set corresponding to those conjugacy classes of non-cyclic subgroups that have a representative lying in D . But all these relations are clearly contained in $\mathcal{Y} \otimes \mathbb{Q}$, so $\mathcal{X} \otimes \mathbb{Q} \subseteq \mathcal{Y} \otimes \mathbb{Q}$ and we are done. \square

`prop:normalbig`

Proposition 3.4. *Let G be a finite group, and $N \triangleleft G$ a normal subgroup of prime index that is either metabelian or supersolvable. If $\Theta = \sum_i n_i H_i$ is a G -relation with all $H_i \leq N$, then Θ is induced from an N -relation.*

Remark 3.5. It is not true that $\sum_i n_i H_i$ is an N -relation, since the H_i are representatives of G -conjugacy classes of subgroups and they might represent the “wrong” N -conjugacy classes. For example, if H_1 and ${}^g H_1$ are not conjugate in N , then $H_1 - {}^g H_1$ will not be an N -relation in general, while it is the zero element in the Burnside ring of G and in particular a G -relation.

Proof. Write p for the index of N in G , and fix a generator T of the quotient $G/N \cong C_p$. Recall (see e.g. [1] §8) that for a C_p -module M ,

$$H^1(C_p, M) = \frac{\text{1-cocycles}}{\text{1-coboundaries}} = \frac{\ker(1 + T + \dots + T^{p-1})}{\text{Im}(1 - T)}.$$

Let $\Theta = \sum_i n_i H_i$ be a G -relation with $H_i \leq N$ for all i ; we view it as an element of the Burnside ring of N . Write $\tilde{\Theta} = \sum m_\rho \rho$ for its image in the rational representation ring $R_{\mathbb{Q}}(N)$, the sum taken over the irreducible³ representations of N . Note that $\text{Ind}_N^G \tilde{\Theta} = 0$, since Θ is a G -relation.

We need to show that we can add to Θ a linear combination of terms of the form ${}^g H - H$ for $H \leq N, g \in G$ such that the resulting element of $B(N)$ is an N -relation. In other words, we claim that Θ is a coboundary for the action of G/N on $M = B(N)/K(N)$; note that G acts naturally on $B(N)$ and $K(N)$, with N acting trivially.

First, observe that the operator $\text{Res}_N^G \text{Ind}_N^G$ on $R_{\mathbb{Q}}(N)$ is, by definition of induction, equal to $1 + T + \dots + T^{p-1}$. Since Θ is a G -relation, $\tilde{\Theta}$ is killed by Ind_N^G , and therefore a fortiori by $1 + T + \dots + T^{p-1}$. In other words $\tilde{\Theta}$ is a 1-cocycle under the action of C_p on the submodule M of $R_{\mathbb{Q}}(N)$.

It remains to prove that

$$H^1(G/N, M) = 0.$$

Any irreducible representation of N is either fixed by G or has orbit of size p . Thus, $R_{\mathbb{Q}}(N)$ as a G/N -module is a direct sum of trivial modules \mathbb{Z} and of regular modules $\mathbb{Z}[C_p]$. The module M , viewed as the image of $B(N)$ in $R_{\mathbb{Q}}(N)$, is of finite index in $R_{\mathbb{Q}}(N)$ by Artin’s induction theorem. Since N is either metabelian or supersolvable, a theorem of Berz [8, 22] says that M is spanned by elements of the form $a_\phi \phi$, as ϕ runs over the irreducible representations of N , for suitable $a_\phi \in \mathbb{N}$. Note that $a_\phi = a_{T\phi}$, because $M \leq R_{\mathbb{Q}}(N)$ is a C_p -submodule. It follows that M is also a direct sum of trivial and of regular C_p -modules. Now $H^1(C_p, \mathbb{Z}) = \text{Hom}(C_p, \mathbb{Z}) = 0$, and also $H^1(C_p, \mathbb{Z}[C_p]) = 0$ since $\mathbb{Z}[C_p] \cong \text{Hom}_{C_p}(\mathbb{Z}[C_p], \mathbb{Z})$ is co-induced. As H^1 is additive in direct sums, we get that $H^1(C_p, M) = 0$, as claimed. \square

³Throughout the proof the word ‘irreducible’ refers to a rational representation, irreducible over \mathbb{Q} .

Definition 3.6. A group is called *p-quasi-elementary* if it has a normal cyclic subgroup whose quotient is a *p*-group. It is called *quasi-elementary* if it is *p*-quasi-elementary for some prime *p*.

prop:biggroup

Proposition 3.7. *Let G be a quasi-elementary group with a proper subgroup D . If $\Theta = \sum_i n_i H_i$ is a G -relation such that $H_i \leq D$ for all i , then it is induced from some proper subgroup of G , and is in particular imprimitive.*

Proof. Write $G = C \rtimes P$, with P a *p*-group and C cyclic of order prime to *p*.

It suffices to prove the proposition for maximal subgroups D of G . Every maximal subgroup of G is either conjugate to $D = C \rtimes S$ with $S \triangleleft P$ of index *p*, or to $D = U \rtimes P$ where U is a maximal subgroup of C . In the former case, $D \triangleleft G$ is of prime index and is quasi-elementary and therefore supersolvable, so the corollary follows from Proposition 3.4. Assume that we are in the latter case. We will show that the map $B(D) \rightarrow B(G)$ is injective, and the claim will follow from Proposition 3.3.

In general, the kernel of the induction map $B(D) \rightarrow B(G)$ is generated by elements of the form $H - {}^g H$ with $H, {}^g H \leq D$. We therefore have to verify that two such $H, {}^g H \leq D = U \rtimes P$ are necessarily D -conjugate.

As $U \triangleleft C$ is maximal, $[C : U] = l$ and $G = C_{l^k} D$ for some prime l and $k \geq 1$. Write $g = cd, c \in C_{l^k}, d \in D$, so ${}^g H = {}^{cd} H$. Replacing H by ${}^d H$ (which is still a subgroup of D), we may assume that $g = c \in C_{l^k}$. If the order of c is less than l^k , then $c \in D$, and we are done. So assume that c has order l^k . If H commutes with C_{l^k} , then $H = {}^c H$, and the claim is trivial. Otherwise, there exists $h \in H$ (without loss of generality of order coprime to l) for which $hch^{-1} = c^i$ for some $i \not\equiv 1 \pmod{l}$. But then ${}^c h h^{-1} = chc^{-1}h^{-1} = c^{1-i}$ still has order l^k , and therefore cannot lie in D , contradicting the assumption that $H, {}^c H \leq D$. \square

cor:smallgpbig

Corollary 3.8. *Let G be a quasi-elementary group and let $\{1\} \neq N_j \triangleleft G$, $N_j \leq D \leq G$, $j = 1, \dots, s$. If $\Theta = \sum_i n_i H_i$ is a G -relation with the property that for each H_i either $N_j \leq H_i$ for some j or $H_i \leq D$, then Θ is imprimitive.*

Proof. Set $\Theta_0 = \Theta$ and define inductively $\Theta_j = \Theta_{j-1} - N_j \Theta_{j-1}$ for $1 \leq j \leq s$. Then Θ_s consists only of subgroups of D , so it is imprimitive by Proposition 3.7. Because the projections $N_j \Theta_{j-1}$ are lifted from G/N_j , they are also imprimitive. \square

lem:ideal

Lemma 3.9. *Let G be a finite group and R any G -relation, possibly 0. Then the \mathbb{Z} -span of all imprimitive relations and R is an ideal in the Burnside ring of G .*

Proof. If $H \neq G$, then $H \cdot \Theta = \text{Ind}^G \text{Res}_H \Theta$ is imprimitive for any relation Θ . If, on the other hand, $H = G$, then $H \cdot \Theta = \Theta$. \square

cor:alaDeligne

Corollary 3.10. *Let G be a finite group and suppose that there exists an imprimitive G -relation R in which G enters with coefficient 1. Then G has no primitive relations.*

Proof. Write $R = G - \sum_{H \leq G} n_H H$. Then $R \cdot \Theta = \Theta - \sum_H n_H \text{Ind}^G \text{Res}_H \Theta$. By Lemma 3.9, $R \cdot \Theta$ is imprimitive, and clearly $\sum_H n_H \text{Ind}^G \text{Res}_H \Theta$ is also a sum of imprimitive relations. \square

4. A CHARACTERISATION IN TERMS OF QUOTIENTS

The main result of this section, Theorem 4.3, gives a characterisation of $\text{Prim}(G)$ in terms of the existence of quasi-elementary quotients of G . First, recall Solomon's induction theorem and a statement complementary to it:

thm:Solomon

Theorem 4.1 (Solomon's induction theorem). *Let G be a finite group. There exists a Brauer relation of the form $G = \sum_H n_H H$ where the sum runs over quasi-elementary subgroups of G and n_H are integers.*

Proof. See [32] Thm. 1 with $\mathbf{K} = \mathbb{Q}$ or [23] Thm. 8.10. \square

thm:Tims

Theorem 4.2 ([14]). *Let G be a non-cyclic p -quasi-elementary group. Then there exists a relation in which G enters with coefficient p . Moreover, in any G -relation the coefficient of G is divisible by p .*

thm:notquasiel

Theorem 4.3. *Let G be a non-quasi-elementary group.*

- (1) $\text{Prim}(G) \cong \mathbb{Z}$ if all proper quotients of G are cyclic.
- (2) $\text{Prim}(G) \cong \mathbb{Z}/p\mathbb{Z}$ if all proper quotients of G are p -quasi-elementary for the same prime p , and at least one of them is not cyclic.
- (3) $\text{Prim}(G) = 0$ otherwise.

In cases (1) and (2), $\text{Prim}(G)$ is generated by any relation in which G has coefficient 1.

Proof. By Solomon's induction theorem, G has a relation of the form $R = G - \sum_{H \neq G} n_H H$, and we claim that R generates $\text{Prim}(G)$ in all cases. By Lemma 3.9, the span I of the set of imprimitive relations and of R is an ideal in $B(G)$. To show that $K(G) \subset I$, let Θ be any relation. Then $\Theta = R \cdot \Theta + (\Theta - R \cdot \Theta)$ and $R \cdot \Theta \in I$. Also,

$$\Theta - R \cdot \Theta = \sum_{H \neq G} n_H (\Theta \cdot H)$$

is imprimitive and therefore also in I . So $\Theta \in I$, as claimed.

It remains to determine the smallest integer $n > 0$ such that G has an imprimitive relation of the form $\Theta = nG - \sum_{H \neq G} m_H H$. Then $\text{Prim}(G) \cong \mathbb{Z}/n\mathbb{Z}$ (and \mathbb{Z} if there is no such n). Clearly G does not enter the relations that are induced from proper subgroups, so such a Θ must be a linear combination of relations lifted from proper quotients.

- (1) If all proper quotients of G are cyclic, there are no such relations.
- (2) If all proper quotients are p -quasi-elementary, then n is a multiple of p by Theorem 4.2, and there is a relation with $n = p$ by the same theorem if one of them is not cyclic.
- (3) Otherwise, either
 - (a) some proper quotient G/N is not quasi-elementary, in which case we apply Solomon's induction to G/N and lift the resulting relation to G ; or
 - (b) G has two proper non-cyclic quotients $G/N_1, G/N_2$ which are p - and q -quasi-elementary with $p \neq q$, in which case we take a linear combination of the two lifted relations $pG + \dots$ and $qG + \dots$.

In both cases, there is an imprimitive relation with $n = 1$, so $\text{Prim}(G) = 0$. \square

cor:quasielquotients

Corollary 4.4. *If a finite group G has a primitive relation, then there is a prime p such that every proper quotient of G is p -quasi-elementary.*

Proof. If G itself is p -quasi-elementary, then so are all its quotients, and there is nothing to prove. Otherwise, apply the theorem. \square

cor:ses

Corollary 4.5. *Let G be a finite group that has a primitive relation. Then G is an extension of the form*

ses

$$(4.6) \quad 1 \rightarrow S^d \rightarrow G \rightarrow Q \rightarrow 1, \quad d \geq 1$$

with S a simple group and Q p -quasi-elementary. Moreover, if S is not cyclic (equivalently if G is not soluble), then the canonical map $Q \rightarrow \text{Out}(S^d)$ is injective and S^d has no proper non-trivial subgroups that are normal in G . In this case, $\text{Prim}(G) \cong \mathbb{Z}$ if Q is cyclic and $\text{Prim}(G) \cong \mathbb{Z}/p\mathbb{Z}$ otherwise.

Proof. By the existence of chief series for finite groups, any $G \neq \{1\}$ is an extension (4.6) of some group Q , with simple S . Because G has a primitive relation, Q is quasi-elementary by Theorem 4.3.

Now suppose S is not cyclic, and consider the kernel K of the map $G \rightarrow \text{Aut}(S^d)$ given by conjugation. The centre of S^d is trivial, so $K \cap S^d = \{1\}$. If $K \neq \{1\}$, then G/K is a proper non-quasi-elementary quotient, contradicting Theorem 4.3. So $G \hookrightarrow \text{Aut}(S^d)$ and, factoring out $S^d \cong \text{Inn}(S^d)$, we get $Q \hookrightarrow \text{Out}(S^d)$. In the same way, if $N \triangleleft G$ is a proper subgroup of S^d , then G/N is not quasi-elementary, so again $N = \{1\}$.

Finally, the description of $\text{Prim}(G)$ is given by Theorem 4.3. \square

rem:nonsolu

Remark 4.7. Conversely, suppose that G is an extension as in (4.6) with p -quasi-elementary Q , non-cyclic S and $Q \hookrightarrow \text{Out}(S^d)$. Suppose also that S^d has no proper non-trivial subgroups that are normal in G . It follows that every non-trivial normal subgroup of G contains S^d . So G is not quasi-elementary but every proper quotient of it is p -quasi-elementary, and therefore G has a primitive relation. This proves Theorem A for all non-soluble groups.

5. PRIMITIVE RELATIONS IN p -GROUPS

sec:pgroups

Definition 5.1. The normal p -rank of a finite group G is the maximum of the ranks of the elementary abelian normal p -subgroups of G .

As in Bouc's work [11], the groups of normal p -rank one will be of particular importance to us. We will repeatedly need the following classification:

prop:prankone

Proposition 5.2 ([20], Ch. 5, Thm. 4.10). *Let P be a p -group with normal p -rank one. Then P is one of the following:*

- the cyclic group $C_{p^n} = \langle c | c^{p^n} = 1 \rangle$;
- the dihedral group $D_{2n+1} = \langle c, x | c^{2^n} = x^2 = 1, xcx = c^{-1} \rangle$ with $n \geq 3$;
- the generalised quaternion group, $Q_{2n+2} = \langle c, x | c^{2^n} = x^2, x^{-1}cx = c^{-1} \rangle$ with $n \geq 1$;
- the semi-dihedral group $SD_{2n+1} = \langle c, x | c^{2^n} = x^2 = 1, xcx = c^{2^{n-1}-1} \rangle$ with $n \geq 3$.

We now present an alternative proof of the Tornehave–Bouc theorem ([11], Cor. 6.16). The ingredients are the results of §3 and a lemma of Bouc [11, Lemma 6.15].

thm:pgroups

Theorem 5.3 (Tornehave–Bouc). *All Brauer relations in p -groups are \mathbb{Z} -linear combinations of ones lifted from subquotients P of the following types:*

item:cpcp

(i) $P \cong C_p \times C_p$ with the relation $1 - \sum_C C + p \cdot P$, the sum taken over all subgroups of order p ;

item:Heisenberg

(ii) P is the Heisenberg group of order p^3 (which is isomorphic to D_8 when $p = 2$), and the relation is $I - IZ - J + JZ$ where $Z = Z(P)$ and I and J are two non-conjugate non-central subgroups of order p ;

item:dih

(iii) $P \cong D_{2^n}$, $n \geq 4$, with the relation $I - IZ - J + JZ$, where $Z = Z(P)$ and I and J are two non-conjugate non-central subgroups of order 2.

Proof. Let P be a p -group that has a primitive relation. By Lemma 3.2, either $P = C_p \times C_p$ or P has cyclic centre. The former case is covered by Example 2.4, so assume that we are in the second case, and let C_p^z be the unique central subgroup of order p .

First, suppose P has normal p -rank $r \geq 2$, with $V = (C_p)^r \triangleleft P$. The conjugation action of P on V is upper-triangular, as is any action of a p -group on an \mathbb{F}_p -vector space. So there are normal subgroups $(C_p)^j \triangleleft G$ for all $j \leq r$, and we denote by E one for $j = 2$. Note that $C_p^z \subset E$, since any normal subgroup of a p -group meets its centre. By [11, Lemma 6.15], any occurrence in a relation of a subgroup that does not contain C_p^z and is not contained in the centraliser $C_P(E)$ of E in P can be replaced by subgroups that either contain C_p^z or are contained in $C_P(E)$, using a relation from a subquotient isomorphic to the Heisenberg group of order p^3 . The remaining relation is then imprimitive by Corollary 3.8. So P has a primitive relation if and only if it is the Heisenberg group of order p^3 .

Now suppose that $r = 1$, so P is as in 5.2. If P is cyclic or generalised quaternion, then every non-trivial subgroup contains C_p^z , so P has no primitive relations by Corollary 3.8. If P is semi-dihedral, then the only conjugacy class of non-trivial subgroups of P that do not contain C_2^z is that of non-central involutions, represented by $\langle x \rangle$, say. But x and C_2^z generate a proper subgroup of P , so P again has no primitive relations by Corollary 3.8. Finally, if P is dihedral of order 2^n , $n \geq 4$, then there are two conjugacy classes of non-trivial subgroups that do not contain C_2^z , represented, say, by I and J . Using the relation in (iii) (cf. [11, page 25]) any occurrence of I in a relation can be replaced by J and by subgroups that contain C_2^z . In the resulting relation, every subgroup will either contain C_2^z or will be contained in $D = C_2^z \times J$, which is a proper subgroup of P . So, applying Corollary 3.8 again, we see that the group of primitive relations of P is generated by the relation of (iii) and the theorem is proved. \square

sec:solvable

6. MAIN REDUCTION IN SOLUBLE GROUPS

thm:mainred

Theorem 6.1. *Every finite soluble group that has a primitive relation is either*

(i) *quasi-elementary, or*

item:serre

(ii) *of the form $(C_l)^d \rtimes Q$, where l is a prime, Q is quasi-elementary and acts faithfully and irreducibly on the \mathbb{F}_l -vector space $(C_l)^d$ by conjugation, or*

item:almostserre

(iii) *of the form $(C_l \rtimes P_1) \times (C_l \rtimes P_2)$, where l, p are primes, and $P_i \hookrightarrow \text{Aut } C_l$ are cyclic p -groups.*

Proof. Since G is soluble and has a primitive relation, by Corollary 4.5 it is an extension of the form

$$(6.2) \quad 1 \rightarrow (C_l)^d \rightarrow G \rightarrow Q \rightarrow 1, \quad d \geq 1,$$

with Q quasi-elementary. We may assume $d \geq 1$ (otherwise we are in (i)) and $Q \neq \{1\}$ (otherwise $G \cong C_l \times C_l$, e.g. by Theorem 5.3, and we are in (iii)). Consider the various possibilities for the structure of Q and its action on $W = (C_l)^d$ by conjugation.

(A) Suppose that l does not divide $|Q|$. The sequence (6.2) then splits by the Schur–Zassenhaus theorem, so $G = W \rtimes Q$. The kernel of the action of Q on W is then a normal subgroup $N \triangleleft G$.

Case 1: $N \neq \{1\}$ and Q is cyclic. By Corollary 4.4, G/N is quasi-elementary. If it is p -quasi-elementary for some $p \neq l$, then its l -part must be cyclic, so $d = 1$. Moreover, since Q/N acts faithfully on C_l , it must be a p -group. So, writing $Q = Q_p \times Q_{p'}$, where Q_p is the Sylow p -subgroup of Q , we deduce that N contains $Q_{p'}$, which is cyclic of order coprime to l , and so $G = (C_l \times Q_{p'}) \rtimes Q_p$ is quasi-elementary (case (i)). If G/N is l -quasi-elementary, then $l \nmid |Q|$ implies that $Q/N \triangleleft G/N$, so $G/N = (Q/N) \times W$. But N is the whole kernel of the action of Q on W , so Q/N must be trivial. In this case $Q = N$ is normal in G , and $G = Q \times W$ is again quasi-elementary.

Case 2: $N \neq \{1\}$ and Q is not cyclic. Write $Q = C \rtimes P$ with C cyclic of order coprime to lp and P a p -group. This time, we know that G/N is p -quasi-elementary by Corollary 4.4. Since $p \neq l$, we have $d = 1$. Also, because G/N is p -quasi-elementary and the action of Q/N on C_l is faithful, Q/N must be a p -group. So N contains C , and $G = (C_l \times C) \rtimes P$ is p -quasi-elementary.

Case 3: $N = \{1\}$ and Q acts reducibly. Since $l \nmid |Q|$, the \mathbb{F}_l -representation W of Q is completely reducible. Say $W = \bigoplus_{i=1}^n V_i$ with irreducible V_i ; so $V_i \triangleleft G$.

Let p be a prime divisor of $|Q|$. A Sylow p -subgroup of Q acts faithfully on W , so it acts non-trivially on one of the V_i , say on V_1 . Because $U = G/(V_2 \oplus \cdots \oplus V_n) \cong V_1 \rtimes Q$ is quasi-elementary by Corollary 4.4, and because its p -Sylow is not normal in it, U must be p -quasi-elementary (and not cyclic). However, Corollary 4.4 asserts that all proper non-cyclic quotients of G are quasi-elementary with respect to the same prime, so $|Q|$ cannot have more than one prime divisor. In other words, Q is a p -group.

Now, both G/V_1 and G/V_2 must be p -quasi-elementary, so their l -parts are cyclic. This is only possible if $n = 2$ and $\dim V_1 = \dim V_2 = 1$. So $W = C_l \times C_l$, and

$$Q \hookrightarrow (\text{Aut } C_l) \times (\text{Aut } C_l) \cong \mathbb{F}_l^\times \times \mathbb{F}_l^\times$$

is an abelian p -group. This is case (iii) of the theorem.

Case 4: $N = \{1\}$ and Q acts irreducibly. This is case (ii).

(B) Suppose that l divides $|Q|$.

Case 5: Q is l' -quasi-elementary for $l' \neq l$. Let \bar{L} be a Sylow l -subgroup of Q . Since $l' \neq l$, \bar{L} is cyclic and normal in Q , and we write $L \triangleleft G$ for its inverse image in G . So G is an extension of $\bar{Q} = Q/\bar{L}$ by L . By the Schur–Zassenhaus theorem it is a split extension, and we may view \bar{Q} as a subgroup of G and consider its conjugation action on L .

If the Frattini subgroup $\Phi(L)$ is trivial, then $L \cong (C_l)^m$ for some m and we are back in case (A) of the proof. So suppose that $\Phi(L) \neq \{1\}$. Then $G/\Phi(L)$ is quasi-elementary by Corollary 4.4.

Assume first that $G/\Phi(L)$ is p -quasi-elementary for $p \neq l$. Then $L/\Phi(L)$ must be cyclic, hence L is cyclic (by a standard property of l -groups). Moreover, $\tilde{Q} = R \rtimes P$ with R cyclic and P a p -group, and $G/\Phi(L) = (L/\Phi(L) \times R) \rtimes P$. Now R acts trivially on $L/\Phi(L)$ and has order prime to l , so R acts trivially on L by the classical theorem of Burnside that the kernel of $\text{Aut}(L) \rightarrow \text{Aut}(L/\Phi(L))$ is an l -group ([20] Ch. 5, Thm. 1.4). It follows that $G = (L \times R) \rtimes P$ and $L \times R$ is cyclic, so G is p -quasi-elementary.

Assume that $G/\Phi(L)$ is l -quasi-elementary. Then \tilde{Q} must be cyclic and normal in $G/\Phi(L)$, and therefore $G/\Phi(L) = L/\Phi(L) \times \tilde{Q}$. Again \tilde{Q} acts trivially on $L/\Phi(L)$, hence on L by Burnside's theorem. It follows that $G = L \times \tilde{Q}$ is l -quasi-elementary.

Case 6: Q is non-cyclic l -quasi-elementary. Now $Q = C \rtimes P$ with C cyclic of order prime to l , and P an l -group, both non-trivial. By Schur-Zassenhaus we may view C as a subgroup of G . Assume that C acts non-trivially on W , for otherwise $C \times W$ is a normal subgroup of G in which C is characteristic, so $C \triangleleft G$ and G is quasi-elementary.

Since $|C|$ and $|W|$ are coprime, W is completely reducible as a representation of C over \mathbb{F}_l . Therefore, the invariant subspace W^C has a (non-trivial) complement on which C acts faithfully. Since W^C is a P -representation, it is a normal subgroup of G . If it is non-zero, then G/W^C is l -quasi-elementary by Corollary 4.4, so the image of C is normal in it. But so is the image of W , so the two commute, contradicting the faithfulness of the action of C on W/W^C . In other words, $W^C = 0$.

Now the inflation-restriction sequence for $C \triangleleft Q$ acting on W reads

$$H^2(Q/C, W^C) \longrightarrow H^2(Q, W) \longrightarrow H^2(C, W).$$

The first group is zero as $W^C = 0$, and the last one is zero as it is killed by $|C|$ and by $|W|$, which are coprime. So the middle group, which classifies extensions of Q by W up to splitting, is zero, in other words $G = W \rtimes Q$ is a split extension.

Next, we show that W is irreducible as a representation of Q . If not, let $0 \subsetneq V \subsetneq W$ be a subrepresentation. Since G/V is l -quasi-elementary (Corollary 4.4 again), C must act trivially on W/V . But, using complete reducibility again, this contradicts the fact $W^C = 0$.

Finally, consider the kernel N of the action of Q on W . As G is a split extension, N may be viewed as a (normal) subgroup of G . If N is non-trivial, G/N is l -quasi-elementary, and so $CN/N \triangleleft G/N$, which implies $CN \triangleleft G$. Moreover, the commutators $[C, W]$ lie both in W and CN , hence in $W \cap CN = \{1\}$. Therefore, W centralises C , so C is normal in G , and it follows that G is l -quasi-elementary. If, on the other hand, N is trivial, then we are in case (ii). \square

rmrk:charSemiDir

Remark 6.3. Before continuing, we recall from [29, §8.2] the classification of irreducible characters of semi-direct products by abelian groups. Let $G = A \rtimes H$ with A abelian. The group H acts on 1-dimensional characters

of A via

$$h(\chi)(a) = \chi(hah^{-1}), \quad h \in H, a \in A, \chi : A \rightarrow \mathbb{C}^\times.$$

Let X be a set of representatives of H -orbits of these characters. For $\chi \in X$ write H_χ for its stabiliser in H . Then χ can be extended to a one-dimensional character of its stabiliser $S_\chi = A \rtimes H_\chi$ in G by defining it to be trivial on H_χ . Let ρ be an irreducible character of $H_\chi \cong S_\chi/A$ and lift it to S_χ . Then $\text{Ind}_{S_\chi}^G(\chi \otimes \rho)$ is an irreducible character of G and all irreducible characters of G arise uniquely in this way, for varying $\chi \in X$ and ρ .

prop:SerreGroups

Proposition 6.4. *Let $G = W \rtimes H$ with $W \cong (C_l)^d$ for $d \geq 2$, and H acting faithfully on W . Let \mathcal{U} be a set of representatives of the G -conjugacy classes of hyperplanes $U \subset W$, and write $H_U = N_H(U)$ for $U \in \mathcal{U}$. Then*

$$\Theta = G - H + \sum_{U \in \mathcal{U}} (H_U U - H_U W)$$

is a G -relation.

Proof. We retain the notation of Remark 6.3 for the irreducible characters of G . Choose the set X of representatives for the H -orbits of 1-dimensional characters of W in such a way that $\ker \chi \in \mathcal{U}$ for $\mathbf{1} \neq \chi \in X$.

To prove that Θ is a relation, it suffices to show that

$$\begin{aligned} \mathbb{C}[G/H] \ominus \mathbf{1} &= \bigoplus_{\chi \in X, \chi \neq \mathbf{1}} \text{Ind}_{S_\chi}^G(\chi \otimes \mathbf{1}_{H_\chi}), \\ \mathbb{C}[G/H_U U] \ominus \mathbb{C}[G/H_U W] &= \bigoplus_{\chi \in X, \ker \chi = U} \text{Ind}_{S_\chi}^G(\chi \otimes \mathbf{1}_{H_\chi}) \quad \text{for } U \in \mathcal{U}. \end{aligned}$$

To do this, first compute the decomposition of $\mathbb{C}[G/T]$ into irreducible characters for an arbitrary $T < G$. The multiplicity $m_{\chi, \rho}^T$ of $\text{Ind}_{S_\chi}^G(\chi \otimes \rho)$ in $\mathbb{C}[G/T]$ is

$$\begin{aligned} m_{\chi, \rho}^T &= \langle \text{Ind}_{S_\chi}^G(\chi \otimes \rho), \text{Ind}_T^G \mathbf{1}_T \rangle_G = \langle \text{Res}_T \text{Ind}_{S_\chi}^G(\chi \otimes \rho), \mathbf{1}_T \rangle_T \\ &= \sum_{x \in S_\chi \backslash G/T} \langle \text{Ind}^{xT} \text{Res}_{S_\chi \cap xT}^{S_\chi}(\chi \otimes \rho), \mathbf{1} \rangle_{xT} \\ &= \sum_{x \in S_\chi \backslash G/T} \langle \text{Res}_{S_\chi \cap xT}(\chi \otimes \rho), \mathbf{1} \rangle_{S_\chi \cap xT}. \end{aligned}$$

Next, take $T = H$. Since $W \subseteq S_\chi$ for each $\chi \in X$, there is a unique double coset in $S_\chi \backslash G/H$, the trivial one. So

$$m_{\chi, \rho}^H = \langle \text{Res}_{H_\chi}^{S_\chi}(\chi \otimes \rho), \mathbf{1}_{H_\chi} \rangle_{H_\chi} = \langle \rho, \mathbf{1}_{H_\chi} \rangle_{H_\chi} = \begin{cases} 1, & \rho = \mathbf{1} \\ 0, & \rho \neq \mathbf{1} \end{cases}$$

as claimed. Finally, for $U \in \mathcal{U}$ we compare $m_{\chi, \rho}^{H_U U}$ and $m_{\chi, \rho}^{H_U W}$.

If $\chi = \mathbf{1}$ and ρ is an irreducible representation of G/W lifted to G , then

$$\begin{aligned} m_{\chi, \rho}^{H_U U} &= \langle \text{Ind}_G^G \mathbf{1}_{H_U U}, \rho \rangle_G = \langle \mathbf{1}, \text{Res}_{H_U U} \rho \rangle_{H_U U} \\ &= \langle \mathbf{1}, \text{Res}_{H_U} \rho \rangle_{H_U} = \langle \text{Ind}_G^G \mathbf{1}_{H_U W}, \rho \rangle_G = m_{\chi, \rho}^{H_U W}. \end{aligned}$$

For $\chi \neq \mathbf{1}$,

$$m_{\chi, \rho}^{H_U U} = \sum_{x \in S_\chi \backslash G/H_U U} \langle \text{Res}_{S_\chi \cap x(H_U U)}(\chi \otimes \rho), \mathbf{1} \rangle_{S_\chi \cap x(H_U U)}.$$

If $\ker \chi \neq U$, or if $\ker \chi = U$ but x represents a non-trivial double coset, then the corresponding summand is 0, since $S_\chi \cap {}^x(H_U U)$ contains ${}^x U$, a hyperplane of W distinct from $\ker \chi$, and the restriction to this hyperplane is a sum of several copies of one non-trivial character. The same is true for $H_U W$. If, on the other hand, $\ker \chi = U$, then $H_\chi \leq H_U$, so that $S_\chi \cap H_U U = H_\chi U$. Therefore

$$m_{\chi, \rho}^{H_U U} = \begin{cases} 1, & \rho = 1 \\ 0, & \rho \neq 1 \end{cases} \quad \text{and} \quad m_{\chi, \rho}^{H_U W} = 0.$$

□

prop:G20

Proposition 6.5. *Let $G = C_l \rtimes H$, with l prime and $H \neq \{1\}$ acting faithfully on C_l . Then $\text{Prim}(G) \cong \mathbb{Z}$. If $H \cong C_{p^k}$ is of prime-power order, then $\text{Prim}(G)$ is generated by*

$$C_{p^{k-1}} - pH - C_l \rtimes C_{p^{k-1}} + pG.$$

If $H \cong C_{mn}$ with coprime $m, n > 1$, then $\text{Prim}(G)$ is generated by

$$G - H + \alpha(C_n - C_l \rtimes C_n) + \beta(C_m - C_l \rtimes C_m),$$

where $\alpha m + \beta n = 1$.

Proof. The existence of the two relations follows immediately from Example 2.3, applied to $\tilde{H} = C_m < H$ and $\tilde{H} = C_n < H$. If H has composite order, the result follows from Theorem 4.3, case (1). If $H \cong C_{p^k}$, then G is p -quasi-elementary, so the coefficient of G in any relation is divisible by p by Theorem 4.2. Clearly, no relation in which G enters with non-zero coefficient can be induced from a subgroup. But also, no such relation can be lifted from a proper quotient, since all proper quotients of G are cyclic and therefore have no non-trivial relations. □

Corollary 6.6. *Theorem A holds for all finite non-quasi-elementary groups.*

Proof. The theorem is already proved for non-soluble groups (Remark 4.7), so suppose G is soluble but not quasi-elementary. Then, if G has a primitive relation, it falls under (ii) or (iii) of Theorem 6.1. This gives one direction.

Conversely, suppose G is of one of these two types, in particular $G \cong (C_l)^d \rtimes Q$, with Q quasi-elementary and acting faithfully on $(C_l)^d$ by conjugation. It is easy to see that every proper quotient of G is quasi-elementary. So Theorem 4.3 combined with Proposition 6.4 for $d \geq 2$ and Proposition 6.5 for $d = 1$ give the asserted description of $\text{Prim}(G)$. □

7. QUASI-ELEMENTARY GROUPS

sec:qegen

In this section, we determine the structure and the representatives of $\text{Prim}(G)$ for quasi-elementary groups that are not p -groups. This is case (4) of Theorem A, and it is by far the most difficult one.

Notation 7.1. For the rest of the section we fix

P	a non-trivial p -group,
C	a non-trivial cyclic group of order coprime to p ,
$G = C \rtimes P$	a quasi-elementary group with normal subgroup C
	and a fixed complementary subgroup $P \leq G$,
$K \triangleleft P$	the kernel of the conjugation action of P on C .

We begin by showing that the presence of primitive relations forces tight restrictions on the structure of K . We then write down generators for $\text{Prim}(G)$ and give necessary and sufficient group-theoretic criteria for these relations to be primitive.

sec:kernel

7.1. The kernel of the conjugation action.

lem:StructOfP

Lemma 7.2. *If P has normal p -rank one or is isomorphic to D_8 , and $K \neq \{1\}$, then G has no primitive relations.*

Proof. By Proposition 5.2, P is either cyclic, generalised quaternion, semi-dihedral, or dihedral. We will consider these cases separately. We may assume that $P \not\cong C_p$, for otherwise $K = P$ and $G = P \times C$ is cyclic. In the remaining cases, we use the notation of Proposition 5.2 for the generators c, x of P . Denote by C_p^z the unique central subgroup of P of order p . Note that K contains C_p^z , since any normal subgroup of a p -group intersects its centre non-trivially.

If P is cyclic or generalised quaternion, then every non-trivial subgroup of P contains C_p^z . So every subgroup of G either contains C_p^z , or contains a non-trivial subgroup of C , or is contained in $D = C_p^z \times C \triangleleft G$. By Corollary 3.8, G has no primitive relations.

If P is semi-dihedral, then there is only one conjugacy class of subgroups of P that do not contain C_2^z , represented by $\langle x \rangle$. Now, up to conjugation, every subgroup of G either contains C_2^z or a non-trivial subgroup of C , or is contained in $D = C \rtimes (C_2^z \times \langle x \rangle) \triangleleft G$. By Corollary 3.8, we are done.

If P is dihedral, then there are two conjugacy classes of non-trivial subgroups of P that intersect $\langle c \rangle$ trivially, I and J , say. They are each generated by a non-central involution. There is a P -relation (cf. Theorem 5.3)

$$I - J - IC_2^z + JC_2^z.$$

Thus, any occurrence of I in any relation can be replaced by groups that either contain C_2^z or are contained in JC_2^z , using a relation that is induced from P , which is a proper subgroup of G . Similarly, any occurrence of $\tilde{C} \rtimes I$ for $\tilde{C} \leq C$ can be replaced by subgroups that either contain C_2^z or are contained in $C \rtimes JC_2^z$ using a relation from a proper subquotient. In summary, by adding imprimitive relations to any given G -relation, all subgroups can be arranged to either contain C_2^z or be contained in $C \rtimes JC_2^z$ and we are again done by Corollary 3.8. \square

lem:normalnoncentral

Lemma 7.3. *Suppose P has a non-central normal subgroup $E \cong C_p \times C_p$ that intersects K non-trivially. Then G has no primitive relations.*

Proof. Since $E \triangleleft P$, the intersection $U = E \cap Z(P)$ is non-trivial. By assumption, U is not the whole of E , so $C_p \cong U \triangleleft P$, and the action of P on E by conjugation factors through a group $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ of order p . In particular, no other $C_p < E$ except for U is normal in P , so every normal subgroup of P that meets E non-trivially must contain U ; hence $U \subset K$. So U commutes both with C and with P , in particular $U \triangleleft G$.

The centraliser $C_P(E)$ of E in P has index p in P . By [11, Lemma 6.15], if H is any subgroup of P that does not contain U and is not contained in $C_P(E)$, then any occurrence of H in a relation can be replaced by subgroups

that either contain $U \leq Z(G)$ or are contained in $C_P(E)$ using a relation induced from P , which is a proper subgroup of G . Similarly, any group of the form $\tilde{C} \rtimes H$ for $\tilde{C} \leq C$ and H as above can be replaced by subgroups that either contain U or are contained in $D = C \rtimes C_P(E)$ using a relation from the quotient G/\tilde{C} . By Corollary 3.8, G has no primitive relations. \square

cor:ZP

Corollary 7.4. *If $K \neq \{1\}$ and P has cyclic centre, then G has no primitive relations.*

Proof. If P has normal p -rank one, we are done by Lemma 7.2. Otherwise P has a normal subgroup $E \cong C_p \times C_p$ (cf. proof of 5.3). Since $Z(P)$ is cyclic, E is not central. Also, both E and K intersect $Z(P)$ non-trivially, so they both contain the unique $C_p \leq Z(P)$, and thus G has no primitive relations by Lemma 7.3. \square

lem:herzog

Lemma 7.5. *Let T be any p -group. Then either $T = \{1\}$ or $T \cong D_8$ or T has normal p -rank one or the number of normal subgroups of T isomorphic to $C_p \times C_p$ is congruent to 1 modulo p .*

Proof. By a Theorem of Herzog [21, Theorem 3], the number α of elements in T of order p is congruent to -1 modulo p^2 if and only if $T \not\cong D_8$ and has normal p -rank greater than one. We consider two cases:

Case 1: $Z(T)$ is cyclic. Since every normal subgroup of T intersects the centre non-trivially and since there is a unique subgroup $\langle z \rangle$ of order p in the centre, any normal $C_p \times C_p$ is generated by z and a non-central element a of order p . For an arbitrary non-central element a of order p , $\langle a, z \rangle$ need not be normal, but the size of its orbit under conjugation is a power of p . So the number of normal such $C_p \times C_p$ is congruent modulo p to the number of all $C_p \times C_p$ that intersect the centre non-trivially. Finally, $p^2 - p$ different non-central elements generate the same subgroup, so the number β of normal subgroups isomorphic to $C_p \times C_p$ is congruent to $(\alpha - (p - 1))/(p^2 - p)$ modulo p . Thus,

$$\begin{aligned} T \not\cong D_8 \text{ and } \exists C_p \times C_p \triangleleft T &\Leftrightarrow \alpha \equiv -1 \pmod{p^2} \\ &\Leftrightarrow \alpha - p + 1 \equiv -p \pmod{p^2} \\ &\Leftrightarrow \beta = \frac{\alpha - (p - 1)}{p^2 - p} \equiv 1 \pmod{p}, \end{aligned}$$

as required.

Case 2: $Z(T)$ is not cyclic. Then a normal subgroup of T isomorphic to $C_p \times C_p$ is either contained in $Z(T)$ or intersects it in a line. Let $Z(T)$ have normal p -rank $r \geq 2$. Any $C_p \times C_p \leq Z(T)$ is generated by two linearly independent elements of order p and there are $(p^r - 1)(p^r - p)/2$ unordered pairs of such elements. Each $C_p \times C_p$ contains $(p^2 - 1)(p^2 - p)/2$ pairs and so there are

$$\frac{(p^r - 1)(p^r - p)}{(p^2 - 1)(p^2 - p)} = \frac{(p^r - 1)(p^{r-1} - 1)}{(p^2 - 1)(p - 1)} \equiv 1 \pmod{p}$$

distinct subgroups of $Z(T)$ that are isomorphic to $C_p \times C_p$. Since there are $p^r - 1 \equiv -1 \pmod{p^2}$ elements in $Z(T)$ of order p , we have by Herzog's theorem that

$$T \not\cong D_8 \text{ and } \exists C_p \times C_p \triangleleft T \Leftrightarrow \#\{g \in T \setminus Z(T) \mid g^p = 1\} \equiv 0 \pmod{p^2}.$$

For any given line in $Z(T)$, the number of $C_p \times C_p \leq T$ intersecting $Z(T)$ in that line is therefore divisible by p by the same counting as in case 1, and so the number of normal $C_p \times C_p$ in T that intersect T in a line is divisible by p , as required. \square

prop:kernelprank1

Proposition 7.6. *Suppose that G has a primitive relation. Then either $K = \{1\}$ or $K \cong D_8$ or K has normal p -rank one. In particular, K has cyclic centre.*

Proof. If K is not of these three types, then by Lemma 7.5, the set of normal $C_p \times C_p$ in K has cardinality coprime to p . The p -group P acts on this set by conjugation, so there is a fixed point. In other words, there is $N = C_p \times C_p \triangleleft K$ that is fixed under conjugation by P , so $N \triangleleft P$. Now, either N is in the centre of P , in which case it is also in the centre of G (since K commutes with C by definition), and G has no primitive relations by Lemma 3.2; or N is a normal non-central subgroup of P that intersects K non-trivially, and then G has no primitive relations by Lemma 7.3. \square

lemcl2

Lemma 7.7. *If $C_{l^2} \leq C$ for some prime l , then $\text{Prim}(G) = 0$.*

Proof. Write $C = C_l^m \times \tilde{C}$ with \tilde{C} cyclic of order prime to l . There is a unique $C_l \triangleleft C$, and any subgroup of G that does not contain it is contained in $\tilde{C} \rtimes P$ and, a fortiori, in $D = (C_l \times \tilde{C}) \rtimes P \subsetneq G$. Since $C_l \triangleleft G$, we are done by Corollary 3.8. \square

not:quasielem

Assumption 7.8. In view of 7.6 and 7.7, from now we assume:

- (1) $G = C \rtimes P$, with P a p -group, and $C = C_{l_1} \times \dots \times C_{l_t}$ cyclic with t distinct primes $l_j \neq p$.
- (2) K is either trivial, or isomorphic to D_8 or has normal p -rank one.

not:CK

Notation 7.9. The following notation will be used in the rest of the section. Here, N is any normal subgroup of G , and j is an index, $1 \leq j \leq t$.

C_p^z	the unique central subgroup of K (and of G) of order p , when K is non-trivial.
C_K	either K if K is cyclic, or a cyclic index 2 subgroup of K that is normal in G otherwise ⁴ ;
\bar{C}_K	CC_K ; this is the largest normal cyclic subgroup of G .
\mathcal{H}_N	a set of representatives of conjugacy classes of subgroups of G that intersect N trivially.
\mathcal{H}_N^c	the set of subgroups of G that intersect N non-trivially.
\mathcal{H}^c	short for $\mathcal{H}_{C_K}^c$.
\mathcal{H}	short for $\mathcal{H}_{\bar{C}_K}$; we take \mathcal{H} to consist of subgroups of P .
\mathcal{H}_m	the set of elements of \mathcal{H} of maximal size.
C^j	$C_{l_1} \times \dots \times \widehat{C_{l_j}} \times \dots \times C_{l_t}$, the l_j' -Hall subgroup of C .
K_j	$\ker(P \rightarrow \text{Aut}(C^j)) = \bigcap_{i \neq j} \ker(P \rightarrow \text{Aut } C_{l_i})$. Thus $K \leq K_j$ and K_j/K is cyclic, as it injects into $\text{Aut } C_{l_j}$.
\tilde{K}_j	$K_j \cap \ker(P \rightarrow \text{Aut } C_K)$.

⁴ If $K \not\cong Q_8$ is non-trivial, then it contains a unique cyclic subgroup of index p , which is normal in G . In Q_8 , there are three cyclic subgroups of index 2 and the 2-group P acts on them by conjugation, so this action has a fixed point, which is also normal in G .

For elements $\Theta_1 = \sum_H n_H H$ and $\Theta_2 = \sum_H m_H H$ of the Burnside ring of G , write

$$\Theta_1 \equiv \Theta_2 \pmod{\mathcal{H}_N^c}$$

if $n_H = m_H$ for all $H \in \mathcal{H}_N$.

Note that C_p^z , C_K , \bar{C}_K , C^j , K_j are all normal (even characteristic) in G , and \bar{C}_K is the largest normal cyclic subgroup of G . The quotient $\bar{P} = G/\bar{C}_K$ acts faithfully on \bar{C}_K by conjugation (as seen from the presentation of generalised quaternion, semi-dihedral and dihedral groups in Proposition 5.2), and is therefore abelian. In particular, G is an extension

$$1 \rightarrow \bar{C}_K \rightarrow G \rightarrow \bar{P} \rightarrow 1,$$

of an abelian p -group by a cyclic group. Also, all $H \in \mathcal{H}$ are abelian, as they inject into $G/\bar{C}_K \cong \bar{P}$. Finally, $C_K \leq \tilde{K}_j$, and the quotient $\tilde{K}_j/C_K \hookrightarrow \text{Aut } C_{l_j}$ is cyclic and acts trivially on C_K by conjugation. It follows that every \tilde{K}_j is abelian.

Any relation in which every term contains a non-trivial subgroup of \bar{C}_K is imprimitive by Lemma 3.1. So, to find generators of $\text{Prim}(G)$, we will from now on focus our attention on relations that contain subgroups of P not containing C_p^z , or, equivalently, subgroups $H \in \mathcal{H}$.

sec:somerels

7.2. Some Brauer relations. In this subsection, we define several relations, which will later be shown to generate $\text{Prim}(G)$.

lem:faithfulchar

Lemma 7.10. *Let $H \in \mathcal{H}$ and let ϕ be a faithful irreducible character of \bar{C}_K . Then $\text{Ind}_{\bar{C}_K}^G \phi$ is irreducible and any irreducible character of G whose restriction to \bar{C}_K is faithful is of this form. Moreover,*

$$\langle \text{Ind}_H^G \mathbf{1}, \text{Ind}_{\bar{C}_K}^G \phi \rangle = \frac{|\bar{P}|}{|H|}.$$

Proof. Since $\bar{P} = G/\bar{C}_K$ acts faithfully on \bar{C}_K , it also acts faithfully on the faithful characters of \bar{C}_K . By Mackey's formula,

$$\langle \text{Ind}_{\bar{C}_K}^G \phi, \text{Ind}_{\bar{C}_K}^G \phi \rangle = \langle \phi, \text{Res}_{\bar{C}_K}^G \text{Ind}_{\bar{C}_K}^G \phi \rangle = \sum_{g \in \bar{C}_K \backslash G/\bar{C}_K} \langle \phi, {}^g \phi \rangle = 1,$$

i.e. $\text{Ind}_{\bar{C}_K}^G \phi$ is irreducible. Moreover, if χ is any irreducible character of G whose restriction to \bar{C}_K is faithful, then by Clifford theory, all irreducible summands of $\text{Res}_{\bar{C}_K}^G \chi$ lie in one orbit under the action of G . Since any normal subgroup of \bar{C}_K is characteristic, all G -conjugate irreducible characters of \bar{C}_K have the same kernel, so all irreducible summands of $\text{Res}_{\bar{C}_K}^G \chi$ are faithful. Thus, if ϕ is one of them, then $\chi = \text{Ind}_{\bar{C}_K}^G \phi$ by Frobenius reciprocity and by the first part of the lemma.

The rest of the lemma now follows by Mackey's formula:

$$\begin{aligned}
\langle \text{Ind}_H^G \mathbf{1}, \text{Ind}_{\bar{C}_K}^G \phi \rangle &= \langle \mathbf{1}, \text{Res}_H \text{Ind}_{\bar{C}_K}^G \phi \rangle \\
&= \langle \mathbf{1}, \sum_{x \in H \backslash G / \bar{C}_K} \text{Ind}_{x \bar{C}_K \cap H}^H \text{Res}_{x \bar{C}_K \cap H}^x \phi \rangle \\
&= \sum_{x \in H \backslash G / \bar{C}_K} \langle \mathbf{1}, \text{Ind}_{\{1\}}^H \text{Res}_{\{1\}}^x \phi \rangle \\
&= \sum_{x \in H \backslash G / \bar{C}_K} \langle \mathbf{1}, \text{Ind}_{\{1\}}^H \mathbf{1} \rangle = |H \backslash G / \bar{C}_K| = \frac{|\bar{P}|}{|H|}.
\end{aligned}$$

□

lem:Clifford

Lemma 7.11. *Let G be any finite group, $N \triangleleft G$ a normal subgroup, and $\Theta_0 = \sum_{H \in \mathcal{H}_N} n_H H \in B(G)$. For an element Λ of $B(G)$ write $\tilde{\Lambda} \in R_{\mathbb{Q}}(G)$ for the associated representation.*

item:Clifford

(1) *For any irreducible character ϕ of G ,*

$$\langle \text{Ind}_N^G \mathbf{1}, \phi \rangle = \begin{cases} \dim \phi, & N \leq \ker \phi \\ 0, & \text{otherwise} \end{cases}.$$

item:HvsHN

(2) *If ϕ is an irreducible character of G satisfying $N \leq \ker \phi$, then for every subgroup $H \leq G$,*

$$\langle \text{Ind}_H^G \mathbf{1}, \phi \rangle = \langle \text{Ind}_{HN}^G \mathbf{1}, \phi \rangle.$$

In particular, $\langle \phi, \tilde{\Lambda} - \widetilde{N\Lambda} \rangle = 0$ for every $\Lambda \in B(G)$.

item:deflations

(3) *Let N_1, \dots, N_r be a collection of non-trivial normal subgroups of G . Set $\Theta_i = \Theta_{i-1} - N_i \Theta_{i-1}$ for $i = 1, \dots, r$. If ϕ is an irreducible character of G whose kernel contains some N_i , then $\langle \tilde{\Theta}_r, \phi \rangle = 0$.*

item:Ncyclic

(4) *Suppose that N is cyclic. If Θ is a relation and $\Theta \equiv \Theta_0 \pmod{\mathcal{H}_N^c}$, then $\langle \tilde{\Theta}_0, \phi \rangle = 0$ for every irreducible character ϕ of G whose restriction to N is faithful.*

item:Thetar

(5) *Suppose that N is cyclic. Let N_1, \dots, N_r and $\Theta_1, \dots, \Theta_r$ be as in part (3), and assume in addition that all N_i are contained in N , and that any normal subgroup of G that intersects N non-trivially contains some N_i . Then $\langle \tilde{\Theta}_r, \phi \rangle = \langle \tilde{\Theta}_0, \phi \rangle$ for every irreducible character ϕ of G that is faithful on N . In particular, Θ_r is a relation if and only if $\langle \tilde{\Theta}_0, \phi \rangle = 0$ for every such character.*

Proof. We implicitly rely on Frobenius reciprocity throughout the proof.

- (1) By Clifford theory, $\text{Res}_N^G \phi$ is a sum of irreducible characters of N that all lie in one G -orbit. The claim follows from the fact that the trivial character is a G -orbit in itself.
- (2) The assumptions imply that the H -invariants of the underlying vector space of ϕ is the same as the HN -invariants, since the entire vector space is N -invariant.
- (3) The operators $\Lambda \mapsto \Lambda - N_i \Lambda$ on $B(G)$ commute pairwise. So Θ_r is of the form $\Theta - N_i \Theta$ for some $\Theta \in B(G)$, and the claim follows from part (2).
- (4) Let ϕ be faithful on N , and let $U \in \mathcal{H}_N^c$. Since N is normal in G and cyclic, $U \cap N \neq \{1\}$ is normal in G , so by part (1), $\langle \text{Ind}_{U \cap N}^G \mathbf{1}, \phi \rangle = 0$. Also, $\text{Ind}_U^G \mathbf{1}$ is a direct summand of $\text{Ind}_{U \cap N}^G \mathbf{1}$, so $\langle \text{Ind}_U^G \mathbf{1}, \phi \rangle = 0$. It follows that $\langle \tilde{\Theta}_0, \phi \rangle = \langle \tilde{\Theta}, \phi \rangle = 0$.

- (5) Suppose ϕ is faithful on N , and hence on each N_i . Then for any $H \leq G$, $\text{Ind}_{HN_i}^G \mathbf{1}$ is a direct summand of $\text{Ind}_{N_i}^G \mathbf{1}$, and $\langle \text{Ind}_{N_i}^G \mathbf{1}, \phi \rangle = 0$ by part (1). We deduce that $\langle \text{Ind}_{HN_i}^G \mathbf{1}, \phi \rangle = 0$, and therefore $\langle \tilde{\Theta}_r, \phi \rangle = \langle \tilde{\Theta}_0, \phi \rangle$, as claimed. For the last claim, if ϕ is not faithful on N then by assumption, $\ker \phi$ contains some N_i , and the assertion follows from part (3).

□

cor:relmodC

Corollary 7.12. *Let $H_i \in \mathcal{H}$ and $\Theta_0 = \sum n_i H_i \in B(G)$. For $1 \leq j \leq t$ set $\Theta_j = \Theta_{j-1} - C_{l_j} \Theta_{j-1}$, and set $\Theta_{t+1} = \Theta_t$ if K is trivial and $\Theta_{t+1} = \Theta_t - C_p^z \Theta_t$ otherwise. In other words,*

$$\Theta_{t+1} = \sum_i n_i \sum_{U \leq \bar{C}_K} \mu(|U|) H_i U,$$

where μ denotes the Moebius function, and U runs over all subgroups of \bar{C}_K . Then the following are equivalent:

item:thetat

(1) Θ_{t+1} is a relation.

item:nis

(2) $\sum \frac{n_i}{|H_i|} = 0$.

item:theta

(3) There exists a relation Θ such that $\Theta \equiv \Theta_0 \pmod{\mathcal{H}^c}$.

Proof. For an element Λ of $B(G)$, denote its image in $R_{\mathbb{Q}}(G)$ by $\tilde{\Lambda}$.

By Lemma 7.11 (5), part (1) is equivalent to the statement that $\langle \tilde{\Theta}_{t+1}, \phi \rangle = 0$ for all irreducible characters ϕ of G that are faithful on \bar{C}_K . So the equivalence with (2) follows from Lemma 7.10.

The equivalence of (1) and (3) follows from Lemma 7.11 (4) and (5): indeed, if there exists a relation $\Theta \equiv \Theta_0 \pmod{\mathcal{H}^c}$, then by Lemma 7.11 (4), $\langle \tilde{\Theta}_0, \phi \rangle = 0$ for all irreducible characters ϕ of G whose restriction to \bar{C}_K is faithful. But then Lemma 7.11 (5) implies that Θ_{t+1} is a relation. □

cor:relmodC2

Corollary 7.13. *Let $H_1, H_2 \in \mathcal{H}$.*

(1) *If $|H_1| = |H_2|$, then there is a relation $\Theta \equiv H_1 - H_2 \pmod{\mathcal{H}^c}$.*

(2) *If $|H_2| = p|H_1|$, then there is a relation $\Theta \equiv H_1 - pH_2 \pmod{\mathcal{H}^c}$.*

thm:sameInters

Theorem 7.14. *Fix an index $1 \leq j \leq t$. For subgroups $H_1, H_2 \in \mathcal{H}$ of the same size, the following are equivalent:*

(1) *There exists a relation $\Theta \equiv H_1 - H_2 \pmod{\mathcal{H}^c}$ that is induced from $C^j \rtimes P$.*

(2) *The element*

$$\sum_{\substack{U \leq \bar{C}_K \\ C_{l_j} \not\leq U}} \mu(|U|) (H_1 U - H_2 U)$$

of $B(G)$ is a relation.

(3) *$\text{Res}_{\tilde{K}_j}^P (H_1 - H_2 - C_p^z H_1 + C_p^z H_2)$ is a relation.*

(4) *There exists an element $g \in P$ such that the intersections $I_1 = H_1 \cap \tilde{K}_j$ and $I_2 = {}^g H_2 \cap \tilde{K}_j$ are contained in one another, and*

$$[N_P I_1 : I_1] = [N_P I_2 : I_2].$$

Proof. By Lemma 7.11 (applied to $G = C^j P$, $N = C^j C_K$, $\Lambda = H_1 - H_2$), the statements (1) and (2) are equivalent, and both equivalent to the condition that

$$\langle \text{Ind}_{H_1}^G \mathbf{1}, \chi \rangle = \langle \text{Ind}_{H_2}^G \mathbf{1}, \chi \rangle$$

for all irreducible characters χ of G whose restriction to $C^j C_K$, equivalently to $C^j C_p^z$, is faithful. By Lemma 7.10, this is automatically satisfied for those χ whose restriction to \bar{C}_K is faithful. Let χ be an irreducible character of G whose restriction to \bar{C}_K has kernel C_{l_j} . Then by [23, Theorem 6.11],

$$\chi = \text{Ind}_{C\tilde{K}_j}^G \rho$$

for some ρ ; here $C\tilde{K}_j$ is the stabiliser of a constituent of $\text{Res}_{\bar{C}_K} \chi$. Moreover, $\text{Res}_{\tilde{K}_j} \rho$ is irreducible, faithful on C_p^z , and any irreducible character of \tilde{K}_j that is faithful on C_p^z is of the form $\text{Res}_{\tilde{K}_j} \rho$ for some such ρ . For $H = H_1$ or H_2 , we have

$$\begin{aligned} \langle \chi, \text{Ind}_H^G \mathbf{1} \rangle &= \langle \text{Ind}_{C\rtimes \tilde{K}_j}^G \rho, \text{Ind}_H^G \mathbf{1} \rangle = \sum_{C\tilde{K}_j \backslash G/H} \langle \rho, \text{Ind}_{C\tilde{K}_j \cap {}^g H}^{C\tilde{K}_j} \mathbf{1} \rangle \\ &= \sum_{C\tilde{K}_j \backslash G/H} \langle \rho, \text{Ind}_{\tilde{K}_j}^{C\tilde{K}_j} \text{Ind}_{\tilde{K}_j \cap {}^g H}^{\tilde{K}_j} \mathbf{1} \rangle = \sum_{C\tilde{K}_j \backslash G/H} \langle \text{Res}_{\tilde{K}_j} \rho, \text{Ind}_{\tilde{K}_j \cap {}^g H}^{\tilde{K}_j} \mathbf{1} \rangle \\ &= \sum_{\tilde{K}_j \backslash P/H} \langle \text{Res}_{\tilde{K}_j} \rho, \text{Ind}_{\tilde{K}_j \cap {}^g H}^{\tilde{K}_j} \mathbf{1} \rangle = \langle \text{Res}_{\tilde{K}_j} \rho, \text{Res}_{\tilde{K}_j}^P \text{Ind}_H^P \mathbf{1} \rangle. \end{aligned}$$

So (1) and (2) are equivalent to the statement that for any irreducible character ϕ of \tilde{K}_j that is faithful on C_p^z , $\langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_H^P \mathbf{1} \rangle = \langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_{H_2}^P \mathbf{1} \rangle$. This in turn is equivalent to (3), again by Lemma 7.11.

We now prove the equivalence of (1)-(3) to (4). Let ϕ be an irreducible character of \tilde{K}_j , faithful on C_p^z . Its kernel, say N , is then necessarily cyclic. For $H = H_1$ or H_2 , by Lemma 7.11 (1),

$$\langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_H^P \mathbf{1} \rangle = \langle \phi, \sum_{\tilde{K}_j \backslash P/H} \text{Ind}_{{}^g H \cap \tilde{K}_j}^{\tilde{K}_j} \mathbf{1} \rangle = \#\{g \in P/H\tilde{K}_j \mid {}^g H \cap \tilde{K}_j \leq N\}.$$

If ${}^g H \cap \tilde{K}_j \not\leq N$ for all $g \in P$, this is 0. Otherwise, replace H by some ${}^g H$ such that ${}^g H \cap \tilde{K}_j \leq N$ (this does not change $\langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_H^P \mathbf{1} \rangle$). We find

eq:innerprod2

$$\begin{aligned} \langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_H^P \mathbf{1} \rangle &= \#\{g \in P/H\tilde{K}_j \mid g \in N_P(H \cap \tilde{K}_j)\} \\ &= [N_P(H \cap \tilde{K}_j) : H\tilde{K}_j]. \end{aligned} \tag{7.15}$$

This uses the fact that $H\tilde{K}_j$ is contained in $N_P(H \cap \tilde{K}_j)$, since \tilde{K}_j is abelian and therefore normalises its subgroups, and since it is normal in P , so that $H \cap \tilde{K}_j$ is normal in H .

To deduce that (3) implies (4) (or rather the contrapositive), assume without loss of generality that $|H_1 \cap \tilde{K}_j| \geq |H_2 \cap \tilde{K}_j|$. Suppose first that no conjugate of $H_2 \cap \tilde{K}_j$ is contained in $H_1 \cap \tilde{K}_j$. Saturate $H_1 \cap \tilde{K}_j$ to a cyclic subgroup N of \tilde{K}_j with \tilde{K}_j/N cyclic. Then no conjugate of $H_2 \cap \tilde{K}_j$

is contained in N , so if ϕ is an irreducible character of \tilde{K}_j with kernel N , then

$$\langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_{H_2}^P \mathbf{1} \rangle = 0 \neq \langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_{H_1}^P \mathbf{1} \rangle.$$

If instead $[N_P I_1 : I_1] \neq [N_P I_2 : I_2]$, then calculation (7.15) shows that these inner products are not equal whenever they are non-zero.

Conversely, if (4) is satisfied, then above calculation yields

$$\langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_{H_1}^P \mathbf{1} \rangle = \langle \phi, \text{Res}_{\tilde{K}_j}^P \text{Ind}_{H_2}^P \mathbf{1} \rangle$$

for all irreducible characters ϕ of \tilde{K}_j that are faithful on C_p^z . \square

prop:cyclicKj

Proposition 7.16. *Suppose that some K_{j_0} is cyclic and let $\Theta = \sum_{H \leq G} n_H H$ be a relation with $n_H = 0$ for all H that contain $C_{l_{j_0}}$. Then*

$$\sum_{\substack{|H \cap K_{j_0}| \leq p^i \\ HK_{j_0} = P}} n_H \equiv 0 \pmod{p} \quad \forall i \geq 0.$$

Proof. Let $\text{Ind}_{C \rtimes K_{j_0}}^G (\chi \otimes \varphi)$ be an irreducible character of G , where χ is a one-dimensional character of C with kernel $C_{l_{j_0}}$, extended to $C \rtimes K_{j_0}$ as in Remark 6.3, and φ is an irreducible character of K_{j_0} . If $H \leq G$ intersects C^{j_0} non-trivially, then by Lemma 7.11 (1),

$$\langle \text{Ind}_{C \rtimes K_{j_0}}^G (\chi \otimes \varphi), \text{Ind}_H^G \mathbf{1} \rangle = 0,$$

while for any $H \leq P$,

$$\begin{aligned} \langle \text{Ind}_H^G \mathbf{1}, \text{Ind}_{C \rtimes K_{j_0}}^G (\chi \otimes \varphi) \rangle &= \sum_{g \in K_{j_0} \backslash P/H} \langle \mathbf{1}_{K_{j_0} \cap {}^g H}, \text{Res}_{K_{j_0} \cap {}^g H}^{K_{j_0}} \varphi \rangle \\ &= \sum_{g \in K_{j_0} \backslash P/H} \langle \mathbf{1}_{g(K_{j_0} \cap H)}, \text{Res}_{g(K_{j_0} \cap H)}^{K_{j_0}} \varphi \rangle \\ &= \#(K_{j_0} \backslash P/H) \cdot \langle \mathbf{1}_{K_{j_0} \cap H}, \text{Res}_{K_{j_0} \cap H}^{K_{j_0}} \varphi \rangle. \end{aligned}$$

The last two equalities follow from the facts that

- (1) $K_{j_0} \triangleleft P$, so that ${}^g(K_{j_0} \cap H) = K_{j_0} \cap {}^g H$ is a subgroup of K_{j_0} ,
- (2) K_{j_0} is cyclic, so that ${}^g(K_{j_0} \cap H) = K_{j_0} \cap H$, since both are subgroups of K_{j_0} of the same order.

So by assumption on Θ , we must have

$$(7.17) \quad \sum_{H \leq P} n_H \#(K_{j_0} \backslash P/H) \cdot \langle \mathbf{1}_{H \cap K_{j_0}}, \text{Res}_{H \cap K_{j_0}}^{K_{j_0}} \varphi \rangle = 0$$

for any 1-dimensional character φ of K_{j_0} . By Lemma 7.11 (1),

$$\langle \mathbf{1}_{H \cap K_{j_0}}, \text{Res}_{H \cap K_{j_0}}^{K_{j_0}} \varphi \rangle = \begin{cases} 1, & H \cap K_{j_0} \leq \ker \varphi \\ 0, & \text{otherwise} \end{cases}.$$

Also, $\#(K_{j_0} \backslash P/H)$ is a power of p , since K_{j_0} is normal in P , and it is equal to 1 if and only if $HK_{j_0} = P$. The result now follows by considering equation (7.17) modulo p for φ with increasing kernels. \square

prop:Ptoosmall

Proposition 7.18. *The following conditions are equivalent:*

- (1) P/K is generated by exactly t elements;
- (2) $K_j \supsetneq K$ for $1 \leq j \leq t$;
- (3) P/K acts faithfully on C but does not act faithfully on any maximal proper subgroup of C .

Moreover, if G does not satisfy these conditions, then $\text{Prim}(G) = 0$.

Proof. The equivalence of (2) and (3) is clear. Suppose that for some j , $K_j = K$. Then $P/K = P/K_j$ injects into $\text{Aut}(C^j)$, which has rank $t - 1$, so P/K is generated by less than t elements. Conversely, if $K_j \supsetneq K$ for all j , then any set of elements $\{g_r\}$, $g_r \in K_{j_r} \setminus K$, generates a group of rank t in $\text{Aut}(C)$, since each g_r acts non-trivially on C_{j_r} and trivially on C^{j_r} . So $P/K \leq \text{Aut}(C)$ cannot be generated by less than t elements.

Suppose that G does not satisfy these conditions, let j_0 be such that $K_{j_0} = K$, or equivalently that P/K acts faithfully on C^{j_0} . Then, $G_0 = C^{j_0} \rtimes P$ satisfies Assumption 7.8, so Corollary 7.12 applies to both G and G_0 . Thus there exists a G -relation $\Theta \equiv \sum n_i H_i \pmod{\mathcal{H}^c}$ if and only if there exists a G_0 -relation $\Theta \equiv \sum n_i H_i \pmod{\mathcal{H}_{C_p^z C^{j_0}}^c}$, which can then be induced to an imprimitive G -relation. Here $C_p^z C^{j_0}$ is considered as a normal subgroup of G^0 . So all occurrences of $H \in \mathcal{H}$ in any G -relation can be replaced by groups intersecting \bar{C}_K non-trivially using imprimitive relations, so G has no primitive relations. \square

sec:Ktriv

7.3. Primitive relations with trivial K . As before, we have $G = C \rtimes P$, where C is a cyclic group of order $l_1 \cdots l_t$ for distinct primes $l_i \neq p$, and P is a p -group. Assume throughout this subsection that $K = \{1\}$, that is P acts faithfully on C . In particular, P is abelian and its p -torsion is an elementary abelian p -group of rank at most t .

If $t = 1$, then $\text{Prim}(G)$ has been described in Proposition 6.5, so we assume for the rest of the subsection that $t > 1$. Define \mathcal{M} to be the set of all index p subgroups of P . For each $M \in \mathcal{M}$, define the *signature* of M to be the vector in \mathbb{F}_2^t whose j -th coordinate is 1 if $K_j \subseteq M$ and 0 otherwise.

prop:condsKtriv

Proposition 7.19. *The following properties of G are equivalent:*

- (1) *All $K_j = \bigcap_{i \neq j} \ker(P \rightarrow \text{Aut } C_{l_i})$ have the same, non-trivial image in the Frattini quotient $P/\Phi(P)$ of P .*
- (2) *Each subgroup of P of index p contains either every K_j or none, and both cases occur. In other words, the set of signatures of elements of \mathcal{M} is $\{(1, \dots, 1), (0, \dots, 0)\}$.*

Proof. A subgroup K_j has trivial image in $P/\Phi(P)$ if and only if it is contained in all maximal proper subgroups of P if and only if the signatures of all $M \in \mathcal{M}$ have a 1 in the j -th coordinate. Moreover, K_1, K_2 , say, have different non-trivial images in the Frattini quotient if and only if there are two hyperplanes in $P/\Phi(P)$ containing one but not the other if and only if there are two subgroups in \mathcal{M} with signatures $(1, 0, \dots)$ and $(0, 1, \dots)$. \square

thm:Ktriv

Theorem 7.20. *The group G has a primitive relation if and only if G satisfies the equivalent conditions of Proposition 7.19. If it does, then $\text{Prim}(G) \cong C_p$ and is generated by the relation*

$$\sum_{U \leq C} \mu(|U|)(MU - M'U),$$

where $M, M' \in \mathcal{M}$ have signatures $(1, \dots, 1)$ and $(0, \dots, 0)$, respectively.

The proof will proceed in several lemmata.

lem:generators

Lemma 7.21. *The group $\text{Prim}(G)$ is generated by relations of the form $\Theta \equiv M - M' \pmod{\mathcal{H}_C^c}$, for $M, M' \in \mathcal{M}$.*

Proof. If a relation contains no subgroup of P , then it is imprimitive by Lemma 3.1. Let $\Theta = n_H H + \dots$ be any relation with $H \leq P$ of index at least p^2 . Pick $M \in \mathcal{M}$ that contains H . Filter M by a chain of subgroups, each of index p in the previous, such that at each step, the image in some $\text{Aut}(C_{l_j})$ decreases. By Corollary 7.13, we can replace H by a subgroup H' in this chain and by subgroups intersecting C non-trivially, adding the relation Θ_{t+1} from Corollary 7.12. Moreover, the added relation is induced from a subgroup (since $\langle H, H' \rangle \leq M < P$), so the class in $\text{Prim}(G)$ is unchanged. Next, we claim that each subgroup in the chain can be replaced by (an integer multiple of) its supergroup in the chain and by elements of \mathcal{H}_C^c , using an imprimitive relation. Let $H' \leq H$ be an index p subgroup such that $\text{Im}(H \rightarrow \text{Aut } C_{l_j}) \neq \text{Im}(H' \rightarrow \text{Aut } C_{l_j})$ for some j . Then, the subgroup $C_{l_j} \rtimes H / \ker(H \rightarrow \text{Aut } C_{l_j})$ is a group of the form discussed in Example 2.3, with H' corresponding to \tilde{H} in that example. Lifting the relation of that example from the quotient, H' can be replaced by $p \cdot H$, as claimed. So, in summary, we can replace any $H \leq P$ by elements of \mathcal{M} and subgroups intersecting C non-trivially, without changing the class in $\text{Prim}(G)$.

Also, by Corollary 7.12, the coefficient of P in any relation is divisible by p . So we can again use the relation of Example 2.3, induced from the subquotient $C_{l_1} \rtimes P / \ker(P \rightarrow \text{Aut } C_{l_1})$ (by Proposition 7.18, we may assume that $\ker(P \rightarrow \text{Aut } C_{l_1}) \neq P$).

We have thus shown that we can replace any subgroup of P by a subgroup in \mathcal{M} , without changing the class in $\text{Prim}(G)$. Finally, by using relations $\Theta \equiv M - M' \pmod{C}$, we can replace all subgroups in \mathcal{M} by one of them. But the coefficient of this one must be zero by Corollary 7.12, so the resulting relation is imprimitive. Thus, $\text{Prim}(G)$ is generated by relations $\Theta \equiv M - M' \pmod{\mathcal{H}_C^c}$, as claimed. \square

Lemma 7.22. *Let Θ be a relation of the form $\Theta \equiv M - M' \pmod{\mathcal{H}_C^c}$ with $M, M' \in \mathcal{M}$. Then its order in $\text{Prim}(G)$ divides p .*

Proof. Any occurrence of pM in a relation can be replaced by a proper subgroup of M and groups intersecting C , using the relation from Example 2.3, and similarly for M' . Next, these strictly smaller groups can all be replaced by one group of the same size, as in the proof of Lemma 7.21, using imprimitive relations. The resulting relation is $\equiv 0 \pmod{\mathcal{H}_C^c}$ by Corollary 7.12, and so is imprimitive. \square

lem:commonEntry

Lemma 7.23. *If $M, M' \in \mathcal{M}$ have signatures that agree in some entry, then there is an imprimitive relation $\Theta \equiv M - M' \pmod{\mathcal{H}_C^c}$.*

Proof. Say the signatures agree in the j th entry. If the common entry is 1, then $M \cap K_j = M' \cap K_j = K_j$, and if it is 0, then the intersections are both equal to the unique index p subgroup of K_j . In either case, there is an imprimitive relation of the required form by Theorem 7.14. \square

Lemma 7.24. *If $M, M' \in \mathcal{M}$ have opposite signatures both of which contain 0 and 1, then there is an imprimitive relation $\Theta \equiv M - M' \pmod{\mathcal{H}_C^c}$.*

Proof. Say the signatures of M and M' start $(0, 1, \dots)$ and $(1, 0, \dots)$, respectively. In particular, there exists $g \in K_1 \setminus M$ with $\langle M, g \rangle = P$ and $g^p \in M$ and $h \in K_2 \setminus M'$ with $\langle M', h \rangle = P$ and $h^p \in M'$. Since $M \cap M'$ is of index p in M and in M' , and since $M' = \langle M \cap M', g \rangle$ and similarly for M , the group $\langle M \cap M', gh \rangle$ is in \mathcal{M} and contains neither K_1 nor K_2 , i.e. it has signature $(0, 0, \dots)$. Thus we get the required relation by applying the previous lemma twice. \square

Corollary 7.25. *If there exists $M \in \mathcal{M}$ whose signature contains 0 and 1, then $\text{Prim}(G)$ is trivial. Otherwise, $\text{Prim}(G)$ is generated by any $\Theta \equiv M - M' \pmod{\mathcal{H}_C^c}$ where M and M' have signatures $(0, \dots, 0)$ and $(1, \dots, 1)$, respectively.*

To conclude the proof of Theorem 7.20, it remains to show:

Lemma 7.26. *Suppose that no element of \mathcal{M} has a signature in which both 0 and 1 occur. Let $M, M' \in \mathcal{M}$ have signatures $(0, \dots, 0)$ and $(1, \dots, 1)$, respectively, let $\Theta \equiv M - M' \pmod{\mathcal{H}_C^c}$ be a relation. Then Θ is primitive.*

Proof. Assume for a contradiction that Θ is a sum of relations that are induced and/or lifted from proper subquotients. Then, at least one summand must contain terms in \mathcal{M} with signature $(0, \dots, 0)$ such that the sum of all coefficients of these terms is not congruent to 0 modulo p . Moreover, by Corollary 7.12 (2), this relation must contain either a term in \mathcal{M} with signature $(1, \dots, 1)$, or P . Since no $M \in \mathcal{M}$ contains a normal subgroup of G , this relation cannot be lifted from a proper quotient, so it must be induced from a proper subgroup. Since two distinct groups in \mathcal{M} generate P , this proper subgroup must be of the form $(C_{l_1} \times \dots \times \widehat{C_{l_{j_0}}} \times \dots \times C_{l_t}) \rtimes P$. By Proposition 7.16, applied with $p^i = |K_{j_0}|/p$, the sum of the coefficients of $M \in \mathcal{M}$ with signature $(0, \dots, 0)$ plus the sum of the coefficients of $H \leq P$ that satisfy $HK_{j_0} = P$ and $|H \cap K_{j_0}| \leq |K_{j_0}|/p^2$ is divisible by p . By the same proposition, applied with $p^i = |K_{j_0}|/p^2$, the second sum is divisible by p . We deduce that the sum of the coefficients of $M \in \mathcal{M}$ with signature $(0, \dots, 0)$ is divisible by p , which is a contradiction. \square

sec:Knontriv

7.4. Primitive relations with non-trivial K . Finally, we consider $G = C \rtimes P$, where C is a cyclic group of order $l_1 \cdots l_t$ for distinct primes l_i different from p , P is a p -group and the kernel K of $P \rightarrow \text{Aut } C$ is non-trivial. By Proposition 7.6, if G has a primitive relation, then K must be isomorphic to D_8 or have normal p -rank one, so it is a group of the type described in Proposition 5.2. We will assume this throughout this subsection. Note that in particular, if p is odd, then K must be cyclic.

Recall that \mathcal{H} is the set of subgroups of P that do not contain C_p^z , the unique subgroup of K of order p that is central in G , and \mathcal{H}_m is the set of elements of \mathcal{H} of maximal size.

lem:genKnontriv

Lemma 7.27. *The group $\text{Prim}(G)$ is generated by relations of the form*

$$\Theta = \sum_{\tilde{C} \leq \tilde{C}_K} \mu(|\tilde{C}|)(\tilde{C}H_1 - \tilde{C}H_2),$$

for $H_1, H_2 \in \mathcal{H}_m$.

Proof. By Corollary 7.12, these are indeed G -relations.

Now let Θ be any relation. If no elements of \mathcal{H} occur in it, then Θ is imprimitive by Lemma 3.1. Suppose $H \in \mathcal{H} \setminus \mathcal{H}_m$ occurs in Θ and $H' \in \mathcal{H}$ is such that $|H'| = p|H|$. Set $I_H = \text{Im}(H \rightarrow \text{Aut } C)$, and consider two cases:

(1) $I_H = \text{Im}(P \rightarrow \text{Aut } C)$. Then the assumption that there exists an element of \mathcal{H} of size $p|H|$ implies that $p = 2$, K is dihedral or semidihedral, and P is a direct product of H and K . In particular, H is normal in P . Let C_2^a be a non-central C_2 in K . By inducing the relation of Example 2.4 from the subquotient $HC_2^a C_p^z / H \cong C_2 \times C_2$, we may replace H by strictly bigger groups in \mathcal{H} and by subgroups of P containing C_p^z , without changing the class of Θ in $\text{Prim}(G)$.

(2) $I_H \neq \text{Im}(P \rightarrow \text{Aut } C)$. Let B be an index p subgroup of $\text{Im}(P \rightarrow \text{Aut } C)$ containing I_H . By intersecting H' with the pre-image of B in P if necessary, we can find an index p subgroup H'' in H' such that H and H'' generate a proper subgroup of P . Thus, the relation $\sum_{\tilde{C} \leq \tilde{C}_K} \mu(|\tilde{C}|)(\tilde{C}H - \tilde{C}H'')$ of Corollary 7.13 is induced from a proper subgroup by Proposition 3.7, so that H can be replaced by H'' , which is a subgroup of H' , and by subgroups that intersect \tilde{C}_K non-trivially without changing the class in $\text{Prim}(G)$. By inducing the relation of Example 2.4 from the subquotient $H'C_p^z / H'' \cong C_p \times C_p$ (note that H' is abelian and C_p^z is central, so H'' is indeed normal in the group generated by the two), we may replace H'' by strictly bigger groups in \mathcal{H} and by subgroups of P containing C_p^z .

In summary, any class in $\text{Prim}(G)$ is represented by a relation of the form $\Theta \equiv \sum n_i H_i \pmod{\mathcal{H}^c}$ with $H_i \in \mathcal{H}_m$.

Since $\sum_i n_i = 0$ by Corollary 7.12, the generators of $\text{Prim}(G)$ are as claimed. \square

lem:Fpvs

Lemma 7.28. *The group $\text{Prim}(G)$ is an elementary abelian p -group.*

Proof. By the previous lemma, it suffices to show that for any $H_1, H_2 \in \mathcal{H}_m$,

$$\Theta = p \cdot \sum_{\tilde{C} \leq \tilde{C}_K} \mu(|\tilde{C}|)(\tilde{C}H_1 - \tilde{C}H_2)$$

is imprimitive. Let A be a subgroup of $\text{Im}(P \rightarrow \text{Aut } C)$ of index p and such that for some j , $A \cap \text{Aut } C_{l_j} \neq \text{Im}(P \rightarrow \text{Aut } C_{l_j})$. By intersecting H_1 and H_2 with the pre-image of A in P , we may find subgroups $H_3 \leq H_1$ and $H_4 \leq H_2$ of index p whose image in $\text{Aut } C$ lies in A , and in particular whose image in $\text{Aut } C_{l_j}$ is strictly smaller than that of H_1 and of H_2 , respectively. By inducing the relation of Example 2.3, we may replace pH_1 and pH_2 in Θ by H_3 and H_4 , respectively, and by groups containing C_{l_j} , without changing the class of Θ in $\text{Prim}(G)$. Now, we can replace H_3 by H_4 and by groups intersecting \tilde{C}_K non-trivially, using the relation of Corollary 7.13 (1). Since H_3 and H_4 together generate a proper subgroup of G (it is contained in the pre-image of A in P), the class of Θ in $\text{Prim}(G)$ is still unchanged. But now, the only element of \mathcal{H} appearing in Θ is H_4 , so by Corollary 7.12, it must appear with coefficient 0 and the resulting relation is imprimitive by Lemma 3.1. \square

It only remains to determine the rank of $\text{Prim}(G)$. We will first treat separately the case that $K = C_p^z$ and $K \triangleleft P$ is a direct summand. In this

case, $K_j \cong K \times (\text{cyclic group})$ for every j , and their images in $P/\Phi(P)$ are either C_p or $C_p \times C_p$.

prop:Pdirprod

Proposition 7.29. *Suppose P is a direct product by $K \cong C_p^z$. If some K_j has image C_p in $P/\Phi(P)$ or some K_{j_1}, K_{j_2} have different images in $P/\Phi(P)$, then $\text{Prim}(G)$ is trivial. Otherwise, $\text{Prim}(G) \cong \mathbb{F}_p^{p-2}$.*

Proof. Denote by \cdot^Φ the image of \cdot in the Frattini quotient $P/\Phi(P)$.

Let $H = \langle a_1, \dots, a_r \rangle$ be a complement to K in P , where r is the smallest number of generators of H . If r is less than the number t of prime divisors of $|C|$, then by Proposition 7.18, some K_j is equal to $K \cong C_p$, and so $K_j^\Phi \cong C_p$. Also, by the same proposition, G has no primitive relations, as claimed.

Suppose from now on that $r = t$. Write $K = \langle c \rangle$. The elements of \mathcal{H}_m are precisely the complements of K in P , so they are shifts of H of the form $H_\delta = \langle c^{\delta_1} a_1, \dots, c^{\delta_r} a_r \rangle$ for $\delta = (\delta_1, \dots, \delta_t) \in \mathbb{F}_p^t$.

Step 1. Suppose $K_j^\Phi \cong C_p$ for some j . Then $K_j^\Phi = K^\Phi$, so the intersection of K_j with any H_δ has trivial image in the Frattini quotient, and therefore consists only of p -th powers. For any $H_\delta \in \mathcal{H}_m$, from the explicit description of the generators it follows that $H_\delta \cap K_j = H \cap K_j$, since taking p -th powers kills c . So by Theorem 7.14, there exists an imprimitive relation $\Theta \equiv H - H_\delta \pmod{\mathcal{H}^c}$. Combined with Lemma 7.27, this implies that $\text{Prim}(G)$ is generated by a relation of the form $\Theta \equiv n_H H \pmod{\mathcal{H}^c}$. But $n_H = 0$ by Corollary 7.12, and so $\text{Prim}(G)$ is trivial by Lemma 3.1.

Step 2. Suppose $K_{j_1}^\Phi \neq K_{j_2}^\Phi$, and both are two-dimensional. Then, given any lines $L_1 \leq K_{j_1}^\Phi, L_2 \leq K_{j_2}^\Phi$ distinct from K^Φ , we can lift a hyperplane in $P/\Phi(P)$ that intersect each $K_{j_i}^\Phi$ in L_i for $i = 1, 2$ to an index p -subgroup of P that intersects K trivially. Thus, given any two complements H_1 and H_2 , we can find H_3 such that $H_i \cap K_{j_i} = H_3 \cap K_{j_i}$ for $i = 1, 2$. Thus, there exist imprimitive relations $\Theta_i \equiv H_i - H_3 \pmod{\mathcal{H}^c}$ for $i = 1, 2$ and so, $\text{Prim}(G)$ is trivial by the same argument as in the previous step.

Step 3. From now on, suppose that $K_1^\Phi = \dots = K_t^\Phi \cong C_p \times C_p$. Denote the $p+1$ lines in this quotient by K^Φ, L_1, \dots, L_p . For any $H \in \mathcal{H}_m$, the image $(H \cap K_j)^\Phi$ is one of the lines L_i . This line is the same for all j (any two $L_{i_1} \neq L_{i_2}$ generate K_1^Φ , forcing H to contain K otherwise). Consider the linear map

$$l : K(G) \rightarrow \mathbb{F}_p^p,$$

that takes $H \in \mathcal{H}_m$ to the i th basis vector when $(H \cap K_j)^\Phi = L_i$, and declaring $l(H) = 0$ for $H \notin \mathcal{H}_m$.

We claim that every relation $\Theta \in \ker l$ is imprimitive. To this end, we first modify Θ to get rid of the subgroups that are in \mathcal{H} but not in \mathcal{H}_m . Fix $H \in \mathcal{H}_m$ (a complement to K in P), and let $H_1 \in \mathcal{H} \setminus \mathcal{H}_m$. Then $H_1 \cong A = \text{Im}(H_1 \rightarrow \text{Aut}(C)) \leq \text{Im}(P \rightarrow \text{Aut}(C))$, so intersecting H with the preimage of A in P , we obtain a proper subgroup $H_2 \leq H$ of the same order as H_1 , and such that $\langle H_1, H_2 \rangle \neq P$, since its image in $\text{Aut}(C)$ is contained in A . The relation $\Omega_1 \equiv H_1 - H_2 \pmod{\mathcal{H}^c}$ of Corollary 7.13 (1) is therefore imprimitive, and it clearly lies in the kernel of l . So by adding relations of the type Ω_1 to Θ , we may replace any terms in Θ that lie in \mathcal{H} but not in \mathcal{H}_m by subgroups of H , without changing the class in $\text{Prim}(G)$.

and without changing $l(\Theta)$. Next, given any $\tilde{H} \leq H$, we can obtain an imprimitive relation of the form $\Omega_2 \equiv \tilde{H} - pH \pmod{\mathcal{H}^c}$ by inducing the relation of Corollary 7.13 (2) from the proper subgroup $C \rtimes H$ of G . This relation also lies in the kernel of l . So by adding relations of the type Ω_2 to Θ , we may assume without loss of generality that $\Theta \equiv \sum_{H \in \mathcal{H}_m} n_H H \pmod{\mathcal{H}^c}$.

Let $H_1, H_2 \in \mathcal{H}_m$ be such that their intersection with some K_j has the same image in $P/\Phi(P)$. We claim that this implies that in fact $H_1 \cap K_j = H_2 \cap K_j$. Indeed, K_j is of the form $K_j = C_p^z \times \langle g \rangle$ for some $g \in P$, and each of these intersections is a complement of C_p^z in K_j . There are p such complements, and they all have distinct images in $P/\Phi(P)$. By Theorem 7.14, there is an imprimitive relation $\Omega_3 \equiv H_1 - H_2 \pmod{\mathcal{H}^c}$, which is in the kernel of l . So we may assume without loss of generality that $\Theta \equiv \sum_H n_H H \pmod{\mathcal{H}^c}$, where all H in the sum give rise to different lines L_k in $P/\Phi(P)$. Since Θ is assumed to lie in the kernel of l , we have $p|n_H$ for all H , and so Θ is imprimitive by Lemma 7.28.

Step 4. By Corollary 7.12, the image of l is precisely equal to the hyperplane $V = \{(v_1, \dots, v_p) \mid \sum v_i = 0 \in \mathbb{F}_p\}$ of \mathbb{F}_p^p . By Step 3, $\text{Prim}(G)$ is isomorphic to the quotient of V by the image of the imprimitive relations under l . Let Θ be imprimitive with non-trivial image under l , without loss of generality assume that it is primitive in its own subquotient \bar{G} . Since $l(\Theta) \neq 0$ and since any two groups in \mathcal{H}_m generate all of P , this subquotient is either a quotient of P or of the form $\tilde{C} \rtimes P$, where \tilde{C} is a proper subgroup of C . So, assume that Θ is as described by Theorem 5.3 or by Lemma 7.27.

Suppose first that it is the former. Then $\bar{G} = P/N$ must be isomorphic to $C_p \times C_p$, since P is abelian, and Θ is then lifted from the relation of Example 2.4. Since the projections of all $H \in \mathcal{H}_m$ in this subquotient have the same size, and since we assume that $0 \neq l(\Theta) \in V$, we deduce that the projections of $H \in \mathcal{H}_m$ in this subquotient are cyclic of order p . Moreover, any two distinct $H, H' \in \mathcal{H}_m$ generate all of P , and neither contains C_p^z , so the projection of C_p^z onto this subquotient is non-trivial cyclic, and the other p terms in Θ of size p correspond to distinct elements of \mathcal{H}_m . If g is a lift of a generator of one such cyclic group from \bar{G} to P , and if c is a generator of C_p^z , then the elements of \mathcal{H}_m entering in Θ are $H_i = \langle c^i g \rangle N$, $i = 0, \dots, p-1$. Since the image of c in the Frattini quotient $P/\Phi(P)$ is non-trivial, it follows that the images of $H_i \cap K_j$ in $P/\Phi(P)$ for $i = 0, \dots, p-1$ are either all the same or all distinct. The assumption that $l(\Theta) \neq 0$ then forces the latter, and so $l(\Theta) = (-1, -1, \dots, -1)$.

Now suppose that $\bar{G} = \tilde{C} \rtimes P$, where \tilde{C} is a proper subgroup of C . Then by Theorem 7.14, $\Theta \equiv H_1 - H_2 \pmod{\mathcal{H}_C^c}$ such that $H_1 \cap K_j = H_2 \cap K_j$ for some j . But then $l(\Theta) = 0$, which is a contradiction.

In summary, the image of the imprimitive relations under l is a one-dimensional subspace of V , spanned by $(1, \dots, 1)$, so $\text{Prim}(G) \cong \mathbb{F}_p^{p-2}$, as claimed. \square

thm:Knontriv

Theorem 7.30. *Assume that either $|K| > p$, or P is not a direct product by K . Let \mathcal{H}_m be the set of subgroups of P of maximal size among those that intersect the centre of K trivially. Define a graph Γ whose vertices are*

the elements of \mathcal{H}_m and with an edge between $H_1, H_2 \in \mathcal{H}_m$ if one of the following applies:

- (1) the subgroup generated by H_1 and H_2 is a proper subgroup of P ;
- (2) $t > 1$ and there exists $1 \leq j_0 \leq t$ such that $H_1 \cap \tilde{K}_{j_0} = H_2 \cap \tilde{K}_{j_0}$, where $\tilde{K}_{j_0} = K_{j_0} \cap \ker(P \rightarrow \text{Aut } C_K)$ (recall that C_K is a fixed maximal cyclic subgroup of K that is normal in G , see Notation 7.9);
- (3) the intersection $H_1 \cap H_2$ is of index p in H_1 and in H_2 , and $\langle H_1, H_2 \rangle / H_1 \cap H_2$ is either dihedral, or the Heisenberg group of order p^3 .

Let d be the number of connected components of Γ . Then $\text{Prim}(G) \cong (C_p)^{d-1}$, generated by relations $\Theta = \sum_{\tilde{C} \leq \tilde{C}_K} \mu(|\tilde{C}|)(\tilde{C}H_1 - \tilde{C}H_2)$ for $H_1, H_2 \in \mathcal{H}_m$ corresponding to distinct connected components of the graph.

Proof. The three conditions for when there is an edge between H_1 and $H_2 \in \mathcal{H}_m$ ensure that if H_1 and H_2 lie in the same connected component of the graph Γ , then there is an imprimitive relation $\Theta \equiv H_1 - H_2 \pmod{\mathcal{H}^c}$, by using Proposition 3.7, Theorem 7.14, and by inducing the relations of Theorem 5.3, respectively.

For a subgroup $H \in \mathcal{H}_m$ write $[H]$ for the connected component of Γ that contains H . Note that since the conjugation action of P on its Frattini quotient is trivial, condition (1) ensures that $[H] = [^g H]$ for any $g \in G$. Therefore $[\cdot]$ extends by linearity to a well-defined linear map $B(G) \rightarrow \mathbb{F}_p^d$, defining it to be 0 on the groups not in \mathcal{H}_m . We are interested in its restriction to the space of relations,

$$[\cdot] : K(G) \longrightarrow \mathbb{F}_p^d.$$

By Corollary 7.12, the image of this restriction is the hyperplane $V = \{\mathbf{v} \mid \sum v_i = 0\}$. We will show that this map establishes an isomorphism between V and $\text{Prim}(G)$.

First, we claim that every imprimitive relation is in $\ker[\cdot]$, so that $[\cdot]$ yields a well-defined map

$$[\cdot] : \text{Prim } G \longrightarrow \mathbb{F}_p^{d-1}.$$

Suppose, on the contrary, that $[\Theta] \neq 0$ and Θ is imprimitive. So $\Theta = \sum_i \Theta_i$, where each Θ_i comes from a proper subquotient of G . Without loss of generality, we may assume that each of these summands is primitive in its subquotient. Moreover, using Lemma 7.27 and Theorem 7.20, we may assume further that Θ_i that are induced from p -groups are of the form described in Theorem 5.3, while Θ_i that are induced/lifted from quasi-elementary subquotients that are not p -groups are as described by Proposition 6.5 and by Lemma 7.27.

Because $[\Theta] \neq 0$, some $[\Theta_i] \neq 0$. The entries of $[\Theta_i] \in \mathbb{F}_p^d$ sum up to 0, so at least two of them are non-zero. In particular, Θ_i contains two terms $H_1, H_2 \in \mathcal{H}_m$ from two different connected components of Γ , appearing in Θ_i with non-zero coefficients modulo p . Since both H_i act faithfully on \tilde{C}_K , their intersection does not contain any normal subgroup of G , so Θ_i must be induced from a proper subgroup of G . Since H_1 and H_2 lie in different connected components of Γ , they generate all of P . So Θ_i is either induced from P or from $\tilde{C} \rtimes P$ for a proper non-trivial subgroup \tilde{C} of C .

If Θ_i is induced from P , then it is induced from a subquotient of the form described in Theorem 5.3 and the images of H_1, H_2 are of order p in it. In fact, since $\langle H_1, H_2 \rangle = P$, this subquotient is a quotient. If it is dihedral or a Heisenberg group of order p^3 , then there is an edge between H_1 and H_2 - contradiction. Otherwise, it is isomorphic to $C_p \times C_p$, so $|P| = p|H_1|$. It follows that $K = C_p^z$ and $P = C_p^z \times H_1$, and this case was excluded.

From now on we may assume that Θ_i is induced from a subgroup $\tilde{C} \rtimes P$. Let $\tilde{K} = \ker(P \rightarrow \text{Aut}(\tilde{C}))$. Since H_1, H_2 are abelian and generate P , their intersection is normal in P , and so is $I = \tilde{K} \cap H_1 \cap H_2$. Since the image of C_p^z in \tilde{K}/I is non-trivial, Θ_i cannot be the relation of Proposition 6.5, so it must be as described by Lemma 7.27. Moreover, since Θ_i is primitive in its subquotient, Proposition 7.6 implies that \tilde{K}/I is isomorphic to D_8 or has normal p -rank one. Pick an index j with $\tilde{C} \leq C^j$ and $K_j \leq \tilde{K}$; see Notation 7.9. Then $K_j/K_j \cap I$ is canonically identified with a non-trivial normal subgroup of \tilde{K}/I , and hence is itself isomorphic to D_8 or has normal p -rank one, or is isomorphic to $C_2 \times C_2$, the latter being only possible if $\tilde{K}/I \cong D_8$.

If $K_j/K_j \cap I$ is isomorphic to D_8 or has normal p -rank one, then $\tilde{K}_j/\tilde{K}_j \cap I$ is cyclic, and so $\tilde{K}_j \cap H_1 \cap H_2$ is a maximal (with respect to inclusion) cyclic subgroup of \tilde{K}_j not containing C_p^z . But $\tilde{K}_j \cap H_1 \cap H_2 \leq \tilde{K}_j \cap H_1, \tilde{K}_j \cap H_2$, which are also cyclic and do not contain C_p^z , so necessarily $\tilde{K}_j \cap H_1 = \tilde{K}_j \cap H_2$, and there is therefore an edge between H_1 and H_2 .

Finally, suppose $K_j/K_j \cap I \cong C_2 \times C_2$ and $\tilde{K}/I \cong D_8$. By Proposition 7.18, these two assumptions and the inclusions $\{1\} \leq K \leq K_j \leq \tilde{K}$ force the index $[C : \tilde{C}]$ to be the product of exactly two primes l_j, l_i . In other words, $\tilde{K} = K = C_p^z \cong C_2$, and $\tilde{K}_j/\tilde{K}_j \cap I, \tilde{K}_i/\tilde{K}_i \cap I$ are the two distinct subgroups of D_8 isomorphic to $C_2 \times C_2$. The intersections $H_1 \cap \tilde{K}, H_2 \cap \tilde{K}$ meet C_p^z trivially, so their images in the quotient \tilde{K}/I are either trivial or non-central of order 2. If these images are conjugate, or if at least one of them is trivial, then either $H_1 \cap \tilde{K}_j$ is conjugate to $H_2 \cap \tilde{K}_j$ or $H_1 \cap \tilde{K}_i$ is conjugate to $H_2 \cap \tilde{K}_i$; in both cases, there is an edge between H_1 and H_2 . So suppose their images in $\tilde{K}/I \cong D_8$ are two non-conjugate non-central subgroups of order 2. Say, $H_1 \cap \tilde{K}_j$ becomes isomorphic to C_2 in \tilde{K}/I , and $H_2 \cap \tilde{K}_j$ becomes trivial. Then by [11, Lemma 6.15], applied to the subgroup $E = K_i/K_i \cap I \cong C_2 \times C_2$ of P/I , with $H = H_1/H_1 \cap I$ there exists a subgroup H' of P/I that centralises E , and a relation

$$\tilde{\Omega} = H - H' - HC_p^z + H'C_p^z$$

in P/I . Lifting it to P , we get a relation

$$\Omega = H_1 - H_3 - H_1C_p^z + H_3C_p^z$$

for some $H_3 \in P$. By Corollary 7.12, $H_3 \in \mathcal{H}_m$. We already showed that the existence of such a relation forces H_1 and H_3 to lie in the same connected component. However, $H_2 \cap \tilde{K}_j = I = H_3 \cap \tilde{K}_j$, since no non-central element of D_8 can lie in one $C_2 \times C_2$ and centralise the other one, and so there is an edge between H_2 and H_3 . So in this case $[H_1] = [H_2]$ as well.

Finally, to determine the kernel of

$$\text{eq:primG} \quad (7.31) \quad [\cdot] : \text{Prim } G \longrightarrow \mathbb{F}_p^{d-1},$$

it suffices to evaluate it on linear combinations of the generators of $\text{Prim}(G)$ given by Lemma 7.27. Such a linear combination is mapped to 0 if and only if the coefficients of all $H \in \mathcal{H}_m$ are divisible by p . We deduce by Lemma 7.28 that the map (7.31) is an isomorphism. \square

ex:Cprime

Remark 7.32. This completes the proof of Theorem A in the last remaining case, when $G = C \rtimes P$ is quasi-elementary with P a p -group and C cyclic of order prime to p .

The conditions in Theorem A(4) that describe when such a G has primitive relations are group-theoretic, but they are rather intricate. In the special case that $|C| = l \neq p$ is prime, they can be made completely explicit, and one can list all such G in terms of generators and relations. We refer the interested reader to [5], and just make one remark here.

Suppose that G has a primitive relation. By Proposition 7.6, the kernel K of the action of P on C by conjugation is $\{1\}$, D_8 or has normal p -rank one. Suppose that $\{1\} \neq K \neq P$ (cf. Example 2.3, Lemma 7.2). Write A for the image of P in $\text{Aut } C$. What makes the case $|C| = l$ simpler is that in this case A is cyclic and the sequence

$$\text{KPAseq} \quad (7.33) \quad 1 \rightarrow K \rightarrow P \rightarrow A \rightarrow 1$$

must split; this makes $P = K \rtimes A$ and G not hard to describe by generators and relations.

Indeed, suppose the sequence does not split. If K is cyclic or generalised quaternion, then all subgroups of K contain the central C_p^z , so, using the notation of section 7.4, \mathcal{H} consists of subgroups of P that intersect K trivially. Since there is no subgroup H of P with $H \cap K = \{1\}$ and surjecting onto A (otherwise P would be a semi-direct product of H by K), all subgroups in \mathcal{H} must be contained in the pre-image under $P \rightarrow \text{Aut } C$ of the unique index p subgroup. Thus, there is an edge between any two groups in \mathcal{H}_m , using the notation of Theorem 7.30, and so $\text{Prim}(G) = \{1\}$. Now suppose K is dihedral or semi-dihedral (the latter cannot actually occur), and denote by C_K the unique cyclic index 2 subgroup of K . Since the automorphism of C_K given by any non-central involution of K is not divisible, P not being a semi-direct product by K implies that it is not a semi-direct product by C_K either. Thus, again, there is an index p subgroup of P containing any subgroup of P that does not intersect C_K , so the same argument applies and shows that $\text{Prim}(G) = \{1\}$.

Finally, let us mention that when C has composite order, it may happen that the sequence (7.33) does not split, but G still has primitive relations. The smallest such example that we know is a group G of order $3934208 = 2^{11} \cdot 17 \cdot 113$, with $C = C_{17} \times C_{113}$, $K = C_8$ and $A = C_{16} \times C_{16}$.⁵ Here there are no subgroups in \mathcal{H} mapping onto A , but the images of two elements of

⁵ In Magma, this group may be given by $\text{PolycyclicGroup}\langle a, b, c, d, e, f, g, h, i, j, k, l, m \mid a^2 = f, b^2 = e, c^2 = d, d^2 = h, e^2 = g, f^2 = i, g^2 = k, h^2 = j, i^2 = j^2, k^2 = l^{17}, m^{113}, {}^a c = c \cdot i, {}^b c = c \cdot f, {}^b d = d \cdot i, {}^c e = e \cdot i, {}^b l = l^3, {}^e l = l^9, {}^g l = l^{13}, {}^k l = l^{16}, {}^b m = m^{48}, {}^c m = m^{42}, {}^d m = m^{69}, {}^e m = m^{44}, {}^g m = m^{15}, {}^h m = m^{15}, {}^j m = m^{112}, {}^k m = m^{112} \rangle$

\mathcal{H} may generate the whole of A . This cannot happen when C has prime order.

remcanrel

Remark 7.34. Although there is no a priori preferred representative of any class in $\text{Prim}(G)$, the generators of $\text{Prim}(G)$ in Theorem A for quasi-elementary G are fairly canonical in the following sense. The results of §7 show that in case 4(c) every primitive G -relation $\Theta = \sum_H n_H H$ satisfies the following conditions:

- There exists at least two subgroups H of P of maximal size among those that intersect C_p^z trivially such that $n_H \not\equiv 0 \pmod{p}$.
- The sum of n_H over all such H is $0 \pmod{p}$.
- For any $\tilde{C} \leq C$, there exists a subgroup H of G that intersects \tilde{C} non-trivially and such that $n_H \neq 0$.

Similar remarks apply to the cases 4(a) and 4(b).

8. EXAMPLES

ex:SL2(F3)

Example 8.1. Let $G = \text{SL}_2(\mathbb{F}_3)$. Its Sylow 2-subgroup S is normal in G and is isomorphic to the quaternion group Q_8 . The Sylow 2-subgroup and G itself are the only non-cyclic subgroups of G , so $K(G)$ has rank 2. Since G is not in the list of Theorem A, all its relations come from proper subquotients. By Theorem 5.3, $K(S)$ is generated by the relation lifted from $S/Z(S) \cong C_2 \times C_2$. The only other subquotient of G that has primitive relations is $G/Z(G) \cong A_4$, which is of type 3(a) in Theorem A with Q cyclic. Combining everything we have said and noting that the three cyclic subgroups of order 4 in S are conjugate in G , we see that $K(G)$ is generated by

$$\begin{aligned}\Theta_1 &= C_4 - C_6 - S + G, \\ \Theta_2 &= C_2 - 3C_4 + 2S.\end{aligned}$$

Example 8.2. Let $G = A_5$. Since G is simple, Theorem 4.3 shows that G has a primitive relation and $\text{Prim}(G) \cong \mathbb{Z}$ and is generated by any relation in which G enters with coefficient 1. Using [31, Theorem 2.16(i)] or explicitly decomposing all permutation characters in A_5 into irreducible characters, we find that

$$\Theta = C_2 - C_3 - V_4 + S_3 - D_{10} + G$$

is a relation (of the form predicted by Theorem 4.1). Theorem 4.3 now implies that all Brauer relations in G can be expressed as integral linear combinations of Θ and of relations coming from proper subgroups. The non-cyclic proper subgroups of G are V_4 , S_3 , D_{10} and A_4 and their relations induced to G together with Θ generate $K(G)$.

ex:wreath

Example 8.3. Let $G = C_3 \wr C_4$ be the wreath product of C_3 by C_4 . Then the subspace of \mathbb{F}_3^4 on which C_4 acts trivially is a normal subgroup of G with non-quasi-elementary quotient. Thus, all relations of G are obtained from proper subquotients by Corollary 4.4.

9. AN APPLICATION TO REGULATOR CONSTANTS

s:appl

Let $\Theta = \sum_H n_H H$ be a Brauer relation in a group G . Write

$$\mathcal{C}_\Theta(1) = \prod_H |H|^{-n_H}.$$

This quantity is called the *regulator constant* of the trivial $\mathbb{Z}G$ -module. We refer the reader to [15] §2.2 and [2] §2.2 for the definition of regulator constants for general $\mathbb{Z}G$ -modules and their properties. Note that $\mathcal{C}_\Theta(\mathbf{1})$ is invariant under induction of Θ from subgroups and lifts from quotients (using $\sum n_H = \langle \Theta, \mathbf{1} \rangle = 0$), and that $\mathcal{C}_{\Theta+\Theta'}(\mathbf{1}) = \mathcal{C}_\Theta(\mathbf{1})\mathcal{C}_{\Theta'}(\mathbf{1})$.

As an application of Theorem A, we classify, given a prime number l , all finite groups G that have a Brauer relation Θ with the property that $\text{ord}_l(\mathcal{C}_\Theta(\mathbf{1})) \neq 0$. Here, ord_l denotes the (additive) l -adic valuation of a non-zero rational number. For an example of number theoretic consequences of the theorem, see [4].

thm:regconsttriv

Theorem 9.1. *Let G be a finite group and l a prime number. Then any Brauer relation Θ in G is a sum of a relation Θ' satisfying $\text{ord}_l \mathcal{C}_{\Theta'}(\mathbf{1}) = 0$ and relations from the following list, induced and/or lifted from subquotients $H = \mathbb{F}_l^d \rtimes Q$ of the following form:*

- (1) $d = 1$, $Q = C_{p^{k+1}}$, $p \neq l$ prime, Q acting faithfully on C_l ; $\Theta = C_{p^k} - pQ - C_l \rtimes C_{p^k} + pH$; $\mathcal{C}_\Theta(\mathbf{1}) = l^{-p+1}$.
- (2) $d = 1$, $Q = C_{mn}$ acting faithfully on C_l , $(m, n) = 1$, $m\alpha + n\beta = 1$; $\Theta = H - Q + \alpha(C_n - \mathbb{F}_l \rtimes C_n) + \beta(C_m - \mathbb{F}_l \rtimes C_m)$; $\mathcal{C}_\Theta(\mathbf{1}) = l^{\alpha+\beta-1}$.
- (3) $d > 1$, either Q is quasi-elementary and acts faithfully irreducibly on $(\mathbb{F}_l)^d$, or $H = (C_l \rtimes P_1) \times (C_l \rtimes P_2)$, where P_1, P_2 are cyclic p -groups, $p \neq l$, acting faithfully on the respective C_l ;

$$\Theta = H - Q + \sum_{U \in \mathcal{U}} (U \rtimes N_Q U - \mathbb{F}_l^d \rtimes N_Q U);$$

$\mathcal{C}_\Theta(\mathbf{1}) = l^{|\mathcal{U}|-d}$, where \mathcal{U} is the set of index l subgroups of \mathbb{F}_l^d up to Q -conjugation.

cor:regconstsubquo

Corollary 9.2. *A group G has a Brauer relation Θ with $\text{ord}_l(\mathcal{C}_\Theta(\mathbf{1})) \neq 0$ if and only if it has a subquotient isomorphic either to $C_l \times C_l$ or to $C_l \rtimes C_p$ with C_p of prime order acting faithfully on C_l .*

Proof. If G has a subquotient $C_l \times C_l$, respectively $C_l \rtimes C_p$, then the induction/lift of a relation from Example 2.4, respectively 2.3 is as required. The converse immediately follows from Theorem 9.1, noting that all groups listed there have a subquotient of the required type. \square

We begin by reducing the theorem to soluble groups.

Definition 9.3. Given a prime number l , write \mathbb{Z}_l for the ring of l -adic integers. We call a Brauer relation $\Theta = \sum_H H - \sum_{H'} H'$ in G a \mathbb{Z}_l -isomorphism if

$$\bigoplus_H \mathbb{Z}_l[G/H] \cong \bigoplus_{H'} \mathbb{Z}_l[G/H'],$$

or equivalently (see [7, Lemma 5.5.2]) if

$$\bigoplus_H \mathbb{F}_l[G/H] \cong \bigoplus_{H'} \mathbb{F}_l[G/H'].$$

The following result is a slight strengthening of [7, Theorem 5.6.11]:

thm:Dress

Theorem 9.4 (Dress's induction theorem). *Let G be a finite group and l a prime number. There exists a \mathbb{Z}_l -isomorphism in G of the form*

$$G + \sum_H \alpha_H H, \quad \alpha_H \in \mathbb{Z},$$

the sum taken over those subgroups H of G for which $H/O_l(H)$ is quasi-elementary. Here $O_l(H)$ is the l -core of H (the largest normal l -subgroup).

Sketch of the proof. This is shown in the course of the proof of [7, Theorem 5.6.11], but since the actual statement of the theorem is somewhat weaker, we summarise for the benefit of the reader the main ideas of the proof. It is enough to prove that for any prime number q , there exists a \mathbb{Z}_l -isomorphism in G of the form

$$aG + \sum_H \alpha_H H,$$

where the sum is over subgroups H for which $H/O_l(H)$ is quasi-elementary, $\alpha_H \in \mathbb{Z}$, and $a \in \mathbb{Z}$ is not divisible by q . In other words, it is enough to exhibit suitable elements of $B(G) \otimes \mathbb{Z}_{(q)}$ that become trivial under the natural map $B(G) \otimes \mathbb{Z}_{(q)} \rightarrow R_{\mathbb{F}_l}(G) \otimes \mathbb{Z}_{(q)}$. To do that, one first writes $\mathbf{1} \in B(G) \otimes \mathbb{Z}_{(q)}$ as a sum of primitive idempotents $\mathbf{1} = \sum_H e_H$, which are described in [7, Corollary 5.4.8], with the property that each e_H is induced from $B(H) \otimes \mathbb{Z}_{(q)}$ ([7, Theorem 5.4.10]). One then shows that under the map

$$B(G) \otimes \mathbb{Z}_{(q)} \longrightarrow R_{\mathbb{F}_l}(G) \otimes \mathbb{Z}_{(q)},$$

only those e_H map to non-zero idempotents, for which $H/O_l(H)$ is q -quasi-elementary. Since each e_H is a linear combination of G -sets G/U , $U \leq H$, with coefficients whose denominators are not divisible by q , the result follows. \square

cor:Dress

Corollary 9.5. *Let G be a finite group and l a prime number. Any Brauer relation can be written as a sum of relations induced from soluble subgroups of G and a \mathbb{Z}_l -isomorphism.*

Proof. Let Θ be an arbitrary Brauer relation in G , let $R = \mathbf{1}_G + \sum_H \alpha_H H$ be a \mathbb{Z}_l -isomorphism, as given by Theorem 9.4. In particular, all subgroups H in the sum are soluble. Since the subgroup of $B(G)$ that consists of \mathbb{Z}_l -isomorphisms forms an ideal in $B(G)$, we see that

$$\Theta \cdot R = \Theta + \sum_H \alpha_H \text{Ind}^G \text{Res}_H \Theta$$

is a \mathbb{Z}_l -isomorphism, and the claim is established. \square

Proof of Theorem 9.1. It is easy to see that if R is a \mathbb{Z}_l -isomorphism, then $\text{ord}_l(\mathcal{C}_R(\mathbf{1})) = 0$ (and in fact, the same is true with $\mathbf{1}$ replaced by any finitely generated $\mathbb{Z}[G]$ -module). Thus, Corollary 9.5 reduces the proof of the theorem to the case that G is soluble.

Writing Θ as a sum of primitive relations listed in Theorem A, we see immediately by inspection that the relations Θ' that generate $\text{Prim}(G)$ in the cases 1, 2, and 4 satisfy $\mathcal{C}_{\Theta'}(\mathbf{1}) = 1$. The remaining assertions of the theorem follow from a direct calculation for the generators of $\text{Prim}(G)$ in the case 3. \square

REFERENCES

- [1] M. F. Atiyah, C. T. C. Wall, Cohomology of groups, in J.W.S. Cassels, A. Fröhlich (Eds), Algebraic Number Theory, Academic Press, 1967.
- [2] A. Bartel, Large Selmer groups over number fields, Math. Proc. Cambridge Philos. Soc. 148 (2010), 73–86.
- [3] A. Bartel, On Brauer-Kuroda type relations of S-class numbers in dihedral extensions, J. reine angew. Math. 668 (2012), 211–244.
- [4] A. Bartel, Elliptic curves with p -Selmer growth for all p , Q. J. Math. (to appear), arXiv:1204.1166 [math.NT], 2012.
- [5] A. Bartel, T. Dokchitser, Brauer relations in finite groups II — quasi-elementary groups of order $p^a q$, arXiv:1110.6618, 2011.
- [6] A. Bartel, B. de Smit, Index formulae for integral Galois modules, J. London Math. Soc. (to appear), arXiv:1105.3876 [math.NT], 2011.
- [7] D. J. Benson, Representations and Cohomology I, Cambridge University Press, 1991.
- [8] G. Berz, Permutationsbasen für endliche Gruppen, Ph.D. thesis, Augsburg, 1994 (Zbl 0924.20003).
- [9] W. Bley, R. Boltje, Cohomological Mackey functors in number theory, J. of Number Theory 105 (2004), 1–37.
- [10] R. Brauer, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, Math. Nachr. 4 (1951), 158–174.
- [11] S. Bouc, The Dade group of a p -group, Invent. Math. 164 no. 1 (2006), 189–231.
- [12] D. Burns, On Artin formalism for the conjecture of Bloch and Kato, Math. Res. Lett. (to appear).
- [13] P. Deligne. Les constantes des équations fonctionnelles des fonctions L , In Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 349. (1973) Springer, Berlin, 501–597.
- [14] T. Dokchitser, Solomon’s induction in quasi-elementary groups, J. Group Theory 14 (2011), 49–51.
- [15] T. Dokchitser, V. Dokchitser, Regulator constants and the parity conjecture, Invent. Math. 178 no. 1 (2009), 23–71.
- [16] T. Dokchitser, V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, Annals of Math. 172 no. 1 (2010), 567–596.
- [17] T. Dokchitser, V. Dokchitser, Root numbers and parity of ranks of elliptic curves, J. Reine Angew. Math. 658 (2011), 39–64.
- [18] W. M. Dress, D. R. Kletzing, On prime ideals in representation rings, Math. Z. 133 (1973), 285–300.
- [19] W. Feit, Characters of Finite Groups, W. A. Benjamin New York, 1967.
- [20] W. Gorenstein, Finite Groups, Chelsea, 1968.
- [21] M. Herzog, Counting group elements of order p modulo p^2 , Proceedings of the AMS 66 no. 2 (1977), 247–250.
- [22] I. Hambleton, L. R. Taylor, Rational permutation modules for finite groups, Math. Z. 231 (1999), 707–726.
- [23] I. M. Isaacs, Character theory of finite groups, AMS Chelsea Publishing, 2006.
- [24] E. B. Kahn, The relative Burnside kernel — the elementary abelian case, preprint, arXiv:0809.1450v1 [math.AT], 2008.
- [25] S. Kuroda, Über die Klassenzahlen algebraischer Zahlkörper, Nagoya Math. J. 1 (1950), 1–10.
- [26] R. P. Langlands, On the functional equation of the Artin l -functions, Yale University preprint, 1970.
- [27] J. Ritter, Ein Induktionssatz für rationale Charaktere von nilpotenten Gruppen, J. Reine Angew. Math. 254 (1972), 133–151.
- [28] G. Segal, Permutation representations of finite p -groups, Quart. J. Math. Oxford (2) 23 (1972), 375–381.
- [29] J.-P. Serre, Linear Representations of Finite Groups, GTM 42, Springer-Verlag 1977.
- [30] B. de Smit, Brauer-Kuroda relations for S-class numbers, Acta Arith. 98 no. 2 (2001), 133–146.

- [31] V. Snaith, Explicit Brauer induction, *Invent. Math.* 94 (1988), 455–478.
- [32] L. Solomon, The representation of finite groups in algebraic number fields, *J. Math. Soc. Japan* 13 no. 2 (1961), 144–164.
- [33] J. Tornehave, Relations among permutation representations of p -groups, preprint, 1984.
- [34] C. D. Walter, Kuroda's class number relation, *Acta Arith.* 35 (1979), 41–51.